Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2003-22 *November 3, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 7 and October 30, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Labora-tories[1, 2]	Unix	Acme mini_httpd 1.0 1, 1.0, 1.10-1.16, thttpd 1.0, 1.90 a, 1.95, 2.0-2.23 b1	A Directory Traversal vulnerability exists in the 'Host: header' field of an HTTP request when virtual hosting is enabled, which could let a remote malicious user obtain sensitive information.	**Acme:** http://www.acme.com/software/mini_httpd/mini_httpd-1.18.tar.gz http://www.acme.com/software/thttpd/thttpd-2.24.tar.gz **Debian:** http://security.debian.org/pool/updates/main/t/thttpd/ **SuSE:** Ftp://ftp.suse.com/pub/suse/	thttpd/ mini_httpd Directory Traversal CVE Name: CAN-2002-1562	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Debian Security Advisory, DSA 396-1, October 29, 2003.
[2] SUSE Security Announcement, SuSE-SA:2003:044, October 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Laboratories[3, 4]	Unix	thttpd 2.21b, 2.21, 2.22, 2.23b1	A buffer overflow vulnerability exists due to a boundary error in the 'defang()' function when handling certain input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.acme.com/software/thttpd/thttpd-2.24.tar.gz **Debian:** http://security.debian.org/pool/updates/main/t/thttpd/	thttpd defang() Remote Buffer Overflow CVE Name: CAN-2003-0899	**High**	Bug discussed in newsgroups and websites.
Adiscon GmbH[5]	Windows	Monitor Ware Agent 1.3, S 4.21 SP1, 5.0 beta	A remote Denial of Service vulnerability exists when a malicious user submits multiple excessive syslog messages on the port it listens on (10514/UDP by default).	Hotfixes available at: http://www.adiscon.org/download/MWAgent-hotfix-2003-09-15.zip	WinSyslog Interactive Syslog Server Long Message Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Apache Software Foundation[6]	Unix, MacOS X 10.x	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A vulnerability exists in the 'mod_cgid' module when threaded MPM is used due to the way CGI redirect paths are handled, which could let a malicious user obtain sensitive information or unauthorized access.	Upgrade available at: http://apache.sunsite.ualberta.ca/httpd/httpd-2.0.48.tar.gz	Apache Web Server mod_cgid Module CGI Data Redirection CVE Name: CAN-2003-0789	Medium	Bug discussed in newsgroups and websites.
Apache Software Foundation[7] ***HP releases advisory[8]***	**MacOS X 10.x, Unix**	**Apache 2.0a9, 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47**	**A Denial of Service vulnerability exists because the 'mod_cgi' doesn't handle output to STDERR correctly.**	**Mandrake: http://www.mandrakesecure.net/en/ftp.php** ***Hewlett Packard:*** **http://itrc.hp.com**	**Apache2 MOD_CGI Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Apache Software Foundation[9]	Windows, Unix	Cocoon 2.1, 2.2	A Directory Traversal vulnerability exists in the 'view-source' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information.	Update available at: http://cocoon.apache.org/mirror.cgi	Apache Cocoon Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[3] Texonet Security Advisory, 20030908, October 27, 2003.
[4] Debian Security Advisory, DSA 396-1, October 29, 2003.
[5] SecurityFocus, October 21, 2003.
[6] SecurityFocus, October 29, 2003.
[7] Mandrake Linux Security Update Advisory, MDKSA-2003:096, September 26, 2003.
[8] Hewlett-Packard Company Security Bulletin, HPSBUX0310-285, October 7, 2003.
[9] SecurityTracker Alert, 1007993, October 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[10, 11]	Windows, NT 4.0/2000, Unix, BSD/OS 4.0, MacOS X 10.x	Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.28, 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A buffer overflow vulnerability exists in the 'mod_alias' and 'mod_rewrite' modules due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	**Apache:** http://apache.mirror.secondchapter.info/httpd/apache_1.3.29.tar.gz **Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/ **OpenPKG:** Ftp://ftp.openpkg.org/release	Apache Web Server Buffer Overflow CVE Name: CAN-2003-0542	**High**	Bug discussed in newsgroups and websites.
Apple[12]	MacOS X 10.0, 10.1, 10.2	MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8	A vulnerability exists when core files are created, which could let a malicious user overwrite arbitrary root owned files.	No workaround or patch available at time of publishing.	MacOS X Core File CVE Name: CAN-2003-0877	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[13]	MacOS X 10.0, 10.1, 10.2	MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, MacOS X Server 10.0, 10.2-10.2.8	Vulnerabilities exist due to insecure file permissions, which could let a malicious user modify sensitive files or potentially execute arbitrary code.	No workaround or patch available at time of publishing.	MacOS X Insecure File Permissions Vulnerabilities CVE Name: CAN-2003-0876	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[14]	MacOS X 10.2	MacOS X 10.2-10.2.8	A buffer overflow vulnerability exists when handling large 'argv' values due to insufficient bounds checking, which could let a malicious user cause a Denial of Service.	Updates available at: http://www.apple.com/macosx/	MacOS X Long Argv Value Buffer Overflow CVE Name: CAN-2003-0895	Low	Bug discussed in newsgroups and websites.
Apple[15]	MacOS X 10.3	MacOS X 10.3	A vulnerability exists in the Panther version of the Screen Effects screensaver because keyboard events are processed prior to authentication, which could let a malicious user manipulate the user environment.	No workaround or patch available at time of publishing.	MacOS X Panther Screen Effects	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[10] OpenPKG Security Advisory, penPKG-SA-2003.046, October 28, 2003.
[11] Immunix Secured OS Security Advisory, IMNX-2003-7+-025-01, October 29, 2003.
[12] @stake, Inc. Security Advisory, October 28, 2003.
[13] @stake, Inc. Security Advisory, A102803-1, October 28, 2003.
[14] @stake, Inc. Security Advisory, A102803-3, October 28, 2003.
[15] Secunia Advisory, SA10089, October 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[16]	MacOS X 10.x	MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, MacOS X Server 10.0, 10.2-10.2.8	Apple Mac OS X 10.3 (Panther) has been released to address multiple new and previously known vulnerabilities, which could let a malicious user cause a Denial of Service, obtain elevated privileges, unauthorized access, or execute arbitrary code.	Mac OS X 10.3 (Panther) upgrade is commercially available. It is not currently known if security updates will be backported to Mac OS X 10.2.x (Jaguar).	Mac OS X Multiple Vulnerabilities	Low/ Medium/ **High** **Low of a DoS; Medium if elevated privileges or unauthor-ized access can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Apple[17]	MacOS X 10.3	MacOS X 10.3, MacOS X Server 10.3	A vulnerability exists in the QuickTime Java implementation, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: http://docs.info.apple.com/article.html?artnum=120266	MacOS X Quicktime Java CVE Name: CAN-2003-0871	Medium	Bug discussed in newsgroups and websites.
Atrium Software Interna-tional[18]	Windows NT 4.0/2000, XP	MERCUR Mailserver 3.3, SP1&SP2, 4.0 1, SP1, 4.2, SP1&SP2	A buffer overflow vulnerability exists when handling the 'POP3 AUTH' command, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Update available at: http://www.atrium-software.com/mail%20server/pub/mcr42sp3a.html	Mercur Mailserver 'POP3 AUTH' Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Atrium Software Interna-tional[19]	Windows NT 4.0/2000, XP	MERCUR Mailserver 3.3, SP1&SP2, 4.0.1, SP1, 4.2, SP1&SP2	A buffer overflow vulnerability exists due to an error when handling the 'IMAP AUTH' command, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Update available at: http://www.atrium-software.com/mail%20server/pub/mcr42sp3a.html	Mercur Mailserver 'IMAP AUTH' Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Bajie[20]	Windows, Unix	Java HTTP Server 0.95, zxv4, zxe1, zxe, zxc, 0.95 d	A Cross-Site Scripting vulnerability exists in the demonstration scripts and servlets that are distributed as part of Bajie HTTP Server, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://www.utdallas.edu/~gxz014000/websrv/httpsrv.95zxv4rel.zip	HTTP Server Example Scripts & Servlets Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[16] SecurityFocus, October 29, 2003.
[17] Apple Security Advisory, APPLE-SA-2003-10-28, October 28, 2003.
[18] SecurityFocus, October 25, 2003.
[19] SecurityFocus, October 25 2003.
[20] Bugtraq, October 16, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Bytehoard [21]	Windows, Unix	Bytehoard 0.7	A Directory Traversal vulnerability exists in the 'infolder' parameter in 'index.php' due to insufficient verification, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=90199	Bytehoard Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Bytehoard [22]	Windows, Unix	Bytehoard 0.7, 0.71	A Directory Traversal vulnerability exists in the 'files.inc.php,' which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Bytehoard Files.INC.PHP Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Caucho Technol-ogy[23]	Windows	Resin 2.0b2, 2.0, 2.1, s020711, 2.1.1, 2.1.2	Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist in the 'env.jsp,' 'form.jsp,' 'session.jsp,' and 'tictactoe.jsp' scripts, which could let a remote malicious user execute arbitrary HTML and script code; and vulnerabilities exist in the 'name' and 'comment' fields of 'guestbook.jsp,' which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.caucho.com/resin-3.0/	Resin Multiple HTML Injection and Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Centrinity [24]	Windows, Unix	FirstClass 7.1	An information disclosure vulnerability exists when appending '/Search' to the URL of the server, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FirstClass HTTP Server Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Charles Stein-kuehler[25]	Unix	sh-httpd 0.3, 0.4	A Directory Traversal vulnerability exists due to insufficient verification of 'GET' and 'POST' requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SH-HTTPD Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[21] SecurityTracker Alert, 1007959, October 20, 2003.
[22] SecurityFocus, October 29, 2003.
[23] E2 Labs Advisory, EXPL-A-2003-026, October 19, 2003.
[24] Secunia Advisory, SA10084, October 29, 2003.
[25] INetCop Security Advisory, 2003-0x82-019, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Chi Kien Uong[26]	Windows, Unix	Guestbook 1.51	Several vulnerabilities exist: an input validation vulnerability exists due to insufficient sanitization of user-supplied data during a message post, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied data when posting an e-mail address or URL to the site, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Guestbook Input Validation & Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the input validation vulnerability and a Proof of Concept exploit has been published for the Cross-Site Scripting vulnerability.
CpCom-merce[27]	Windows, Unix	CpCom-merce 0.5 f	A vulnerability exists because the '_functions.php' file includes some files relevant to the '$prefix' variable, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CPCommerce Functions Remote Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit URL has been published.
Dansie[28]	Windows, Unix	Shopping Cart	An information disclosure vulnerability exists in the 'db' parameter due to insufficient verification, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Shopping Cart Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
DeskPro[29]	Windows, Unix	DeskPro 1.1 .0	Multiple vulnerabilities exist in the 'faq.php' and 'view.php' modules due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.deskpro.com/	DeskPro Multiple SQL Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
e107.org[30]	Windows, Unix	e107 website system 0.545, 0.603	A vulnerability exists in the 'Chatbox.php' script due to improper handling of user-supplied HTML or script code in the 'Name:' field, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	e107 website system Chatbox.php Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[26] Bugtraq, October 26, 2003.
[27] Zone-H Security Team Security Advisory, ZH2003-31SA, October 19, 2003.
[28] Indonesia Security Development Team Advisory, October 19, 2003.
[29] Bugtraq, October 20, 2003.
[30] SecurityTracker Alert, 1008039, October 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Emule-Project.net [31]	Unix	Emule 0.29c	A remote Denial of Service vulnerability exists when a malicious user submits a large number of characters for the 'password' value if the login form.	No workaround or patch available at time of publishing.	Emule Long Password Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Eric Raymond [32, 33, 34]	Unix	Fetchmail 5.9.0, 6.2.4	A Denial of Service vulnerability exists when a malicious user submits a specially crafted e-mail message. Execution of arbitrary code may also be possible	**Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Slackware:** Ftp://ftp.slackware.com/pub/slackware/	Fetchmail Remote Denial of Service CVE Name: CAN-2003-0792	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Erik Dalen[35]	Unix	Music-queue 0.9-0.9.2, 1.0-1.1.1	Multiple buffer overflow vulnerabilities exist due to insufficient bounds checking when passing user-supplied input to the sprintf() libc function, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Musicqueue Multiple Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Erik Dalen[36]	Unix	Music-queue 1.2	A vulnerability exists in a signal handling procedure when a segmentation violation occurs, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	No workaround or patch available at time of publishing.	Musicqueue SIGSEGV Signal Handler Insecure File Creation	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. Exploit script has been published.
Fastream [37]	Windows	NetFile 6.0.3 .588	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from user-supplied URLs when displaying an HTTP 404 (Not Found) error page, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	NetFile Error Message Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi[38]	Windows, Unix	PHP-Nuke 7.0	A path disclosure vulnerability exists in the search field when invalid input is supplied, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Nuke Search Field Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.

[31] Secunia Advisory, SA10049, October 22, 2003.
[32] Mandrake Linux Security Update Advisory, MDKSA-2003:101, October 16, 2003.
[33] Immunix Secured OS Security Advisory, IMNX-2003-7+-023-01, October 20, 2003.
[34] Slackware Security Bulletin, SSA:2003-300-02, October 27, 2003.
[35] INetCop Security Advisory, 2003-0x82-020, October 27, 2003.
[36] INetCop Security Advisory, 2003-0x82-020, October 27, 2003.
[37] Securiteam, October 29, 2003.
[38] Bugtraq, October 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Fuzzy Monkey[39]	Windows, Unix	MyClas-sifieds 2.11	An input validation vulnerability exists in the '$email' variable, which could let a remote user execute arbitrary code.	Upgrade available at: http://www.fuzzymonkey.org/files/myclassifiedssql-2.13.tar.gz	MyClassifieds Email Variable SQL Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Gast Arbeiter[40]	Multiple	Gast Arbeiter 1.3	A vulnerability exists due to insufficient validation of user-supplied input during uploads, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Gast Arbeiter File Upload Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Geeklog[41]	Unix	Geeklog 1.3.8 , rc!&rc2, 1.3.8 -1sr1, 1.3.8 –1	A vulnerability exists in the 'reqid' parameter when updating passwords because a remote malicious user can change the password for arbitrary users.	Upgrade available at: http://www.geeklog.net/filemgmt/singlefile.php?lid=254	Geeklog Password Update Feature	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser, however, a Proof of Concept exploit has been published.
Gernot Stocker[42]	Unix	kpopup 0.9.1, 0.9.5 pre2	Several vulnerabilities exist: a vulnerability exists because certain user input is used in a 'system()' call without being properly verified, which could let a malicious user execute arbitrary commands with root privileges; and format string vulnerabilities exist due to inadequate handling of strings when passed to the program as arguments, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	kpopup Privileged Command Execution & Elevated Privileges	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published for the 'system()' call vulnerability.
Gold Scripts[43]	Unix	GoldLink 3.0	A vulnerability exists due to an input validation error in 'variables.php' when the 'Acceso' function processes user credentials stored in cookies, which could let a malicious user obtain execute arbitrary code and obtain administrative privileges.	No workaround or patch available at time of publishing.	GoldLink Cookie Administrative Privileges	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[39] Securiteam, October 22, 2003.
[40] Bugtraq, October 20, 2003.
[41] Securiteam, October 19, 2003.
[42] Securiteam, October 29, 2003.
[43] Secunia Advisory, SA10047, October 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [44]	Unix	Compaq Tru64 4.0 g PK4 (BL22), 4.0 f PK8 (BL22)	A vulnerability exists due to an error in CDE dtprintinfo, which could let a local/remote malicious user obtain unauthorized access.	Patches available at: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020256-V40GB22-ES-20031010 http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT0020257-V40FB22-ES-20031010	CDE dtprintinfo Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [45]	Unix	HP-UX 11.0, 11.11, 11.23	A vulnerability exists in the Servicecontrol Manager, which could let a malicious user obtain unauthorized access.	Updates available at: http://software.hp.com/	HP Servicecontrol Manager Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [46]	Windows 95/98/ME/ NT 4.0/2000, XP	Insight Manage-ment for Clients 3.5, 4.0, 5.0, Insight Manager LC versions 1.0, 1.60, Remote Diagnostics Enabling Agent	A vulnerability exists in various web agents released with the Management Software, which could let a remote malicious user obtain unauthorized privileges access or cause a Denial of Service.	Upgrades available at: ftp://ftp.compaq.com/pub/softpaq/sp24501-25000/SP24815.exe	Management Software Web Agents Unauthorized Access	Low/ Medium (Medium if access can be obtained)	Bug discussed in newsgroups and websites.
Hewlett Packard Company [47]	Windows NT 4.0/2000, Unix	OpenView Network Node Manager 6.2 , Solaris, NT 4.X/ Windows 2000, HP-UX 11.x, 10.x, 6.4, NT 4.X/ Windows 2000, HP-UX 11.x	Two vulnerabilities exist in the OpenView Network Node Manager (NNM) when handling malformed TCP packets, which could let a remote malicious user cause a Denial of Service.	Patches available at: http://itrc.hp.com	OpenView Network Node Manager Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[44] Hewlett-Packard Company Software Security Response Team, SSRT2405a, October 24, 2003.
[45] Hewlett-Packard Company Security Bulletin, HPSBUX0310-287, October 7, 2003.
[46] Hewlett-Packard Company Software Security Response Team Advisory, SSRT3632, October 21, 2003.
[47] Hewlett-Packard Company Security Bulletin, HPSBUX0310-291, October 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hiroyuki Yama-moto[48]	Unix	Sylpheed 0.9.4-0.9.6, Sylpheed-Claws 0.9.4-0.9.6 claws	A format string vulnerability exists in 'send_message.c' when handling error responses from SMTP servers, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://sylpheed.good-day.net/sylpheed/sylpheed-0.9.7.tar.g Patch available at: http://cvs.sourceforge.net/viewcvs.py/sylpheed-claws/sylpheed-claws/src/send_message.c?r1=1.18&r2=1.19&diff_format=u	Sylpheed-Claws Format String	**High**	Bug discussed in newsgroups and websites.
Infrontech [49]	Windows NT 4.0/2000, Unix	WebTide 7.0 4	A vulnerability exists due to an input validation error when a HTTP request for '%3f.jsp' is submitted, which could let a remote malicious user obtain sensitive information.	Upgrade available at: www.infrontech.com/english/e-product_webtide.jsp	WebTide Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
Intrago Ltd.[50]	Unix	Adelix CensorNet 3.0, 3.1 r6, 3.1 r5, 3.2; Daniel Barron Dans Guardian 2 2.2.4-2.2.10, 2.4.5 –1, 2.6.1 –5, 2.7.3 -1	A Cross-Site Scripting vulnerability exists in the 'dansguardian.pl' script due to insufficient filtering of user-supplied URLs, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DansGuardian Denied URL Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IpSwitch [51] ***Exploit script has been published*** [52]	**Windows**	**WS FTP Server 3.4, 4.0 1**	**A buffer overflow vulnerability exists in the 'APPE' and STAT FTP' commands when handling excessive data, which could let a remote malicious user execute arbitrary code or cause a Denial of Service.**	**No workaround or patch available at time of publishing.**	**WS_FTP Server Buffer Overflow**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.** ***Exploit script has been published.***

[48] Georgi Guninski Security Advisory #61, October 22, 2003.
[49] STG Security Advisory, SSA-20031025-05, October 28, 2003.
[50] Bugtraq, October 22, 2003.
[51] Bugtraq, September 6, 2003.
[52] SecurityFocus, October 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IRCNet[53] *Vendors issue advisories* *54, 55*	Unix	IRCNet IRCD 2.10, 2.10.3 p3	A buffer overflow vulnerability exists in the 'm_join' function due to a boundary error, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: ftp://ftp.irc.org/irc/server/irc2.10.3p4.tgz *Conectiva:* ftp://atualizacoes.conectiva.com.br/9/RPMS/ircd-2.10.3p3-27242U90_2cl.i386.rpm *OpenPKG:* ftp://ftp.openpkg.org/current/SRC/ircd-2.10.3p5-20031013.src.rpm	IRCnet IRCD Buffer Overflow CVE Name: CAN-2003-0864	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
JBoss Group[56] *Upgrade now available* *57*	Windows, Unix	JBoss 3.0.8, 3.2.1	A vulnerability exists in the SQL database 'HSQLDB' used for managing JMS connections due to a combination of various errors in some classes in JDK and insecure default settings, which could let a remote malicious user manipulate data, obtain sensitive information, cause a Denial of Service, or execute arbitrary commands.	Workaround available at: http://sourceforge.net/docman/display_doc.php?docid=19314&group_id=22866 *Upgrade available at:* http://www.jboss.org/index.html?module=html&op=userdisplay&id=downloads	JBoss HSQLDB Remote Command Injection	Low/ Medium/ High Low if a DoS, Medium is sensitive informa-tion can be obtained; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

[53] Bugtraq, October 12, 2003.
[54] Conectiva Linux Security Announcement, CLA-2003:765, October 17, 2003.
[55] OpenPKG Security Advisory, OpenPKG-SA-2003.045, October 19, 2003.
[56] Illegalaccess.org Security Alert, October 5, 2003.
[57] SecurityFocus, October 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE[58, 59 60, 61, 62] ***More advisories issued***[63, 64]	**Unix**	**KDE 1.1-1.1.2, 1.2, 2.0 BETA, 2.0- 2.2.2, 3.0- 3.0.5, 3.1- 3.1.3**	**Two vulnerabilities exist: a vulnerability exists in the KDE Display Manager (KDM) when used in combination with Pluggable Authentication Modules (PAM), which could let an unauthorized remote malicious user obtain root access; and a vulnerability exists due to a weak session cookie algorithm that does not fully use the available 128 bits of entropy, which could let a remote malicious user obtain system access.**	**Patches available at:** ftp://ftp.kde.org/pub/kde/security_patches **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** Http://security.debian.org/pool/updates/main/k/kdebase/ **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **RedHat:** ftp://updates.redhat.com/ ***SGI:*** http://www.sgi.com/support/security/ ***TurboLinux:*** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/8/updates/	**KDM PAM Module PAM_SetCred Privilege Escalation** **CVE Names: CAN-2003-0690, CAN-2003-0692**	**High**	**Bug discussed in newsgroups and websites.**
Khaled Mardam-Bey[65]	Windows	mIRC 6.1	A buffer overflow vulnerability exists due to a boundary error when a browser passes input to mIRC via the 'irc:' URI handler, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.mirc.com/get.html	mIRC IRC URL Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Khaled Mardam-Bey[66] ***Upgrade now available***[67]	**Windows**	**mIRC 6.1, 6.11**	**A buffer overflow vulnerability exists in 'DCC SEND' requests due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service.**	***Upgrade available at:*** http://www.mirc.com/get.html	**mIRC 'DCC SEND' Buffer Overflow**	**Low**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Khaled Mardam-Bey[68]	Windows	mIRC 6.12	A buffer overflow vulnerability exists in 'DCC SEND" requests when a filename is of excessive length and contains certain characters, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	mIRC DCC SEND Variant Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[58] KDE Security Advisory, September 16, 2003.
[59] Red Hat Security Advisory, RHSA-2003:269-01, September 16, 2003.
[60] Mandrake Linux Security Update Advisory, MDKSA-2003:091, September 17, 2003.
[61] Conectiva Linux Security Announcement, CLA-2003:747, September 19, 2003.
[62] Debian Security Advisory, DSA 388-1, September 19, 2003.
[63] Turbolinux Security Advisory, TLSA-2003-59, October 20, 2003.
[64] SGI Security Advisory, 20031002-01-U, October 27, 2003.
[65] NTBugtraq, October 15, 2003.
[66] Secunia Advisory, SA10000, October 13, 2003.
[67] Bugtraq, October 18, 2003.
[68] Bugtraq, October 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media[69]	Multiple	Director MX 5.0, Flash 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0, 6.0.65.0, 6.0.79.0	A vulnerability exists because '.sol' files are stored in a predictable location on client systems, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Macromedia Flash Player Flash Cookie Predictable File Location	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Martin K. Peterson[70, 71, 72]	Unix	GDM 2.2.5.4, 2.4.1, 2.4.1.1-2.4.1.6, 2.4.4	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when a malicious user submits an arbitrary number of bytes to GDM; and a Denial of Service vulnerability exists due to a failure to impose a timeout when queering for certain commands.	Upgrade available at: http://ftp.gnome.org/pub/GNOME/sources/gdm/2.4/ **Conectiva:** Ftp://atualizacoes.conectiva.com.br/ **Mandrake:** Http://www.mandrakesecure.net/en/ftp.php **Slackware:** ftp://ftp.slackware.com/pub/slackware/	Multiple GDM Denial of Service CVE Names: CAN-2003-0793, CAN-2003-0794	Low	Bug discussed in newsgroups and websites.
Microsoft[73] ***Microsoft updates bulletin & exploit script published***[74]	**Windows NT 4.0/2000**	**Exchange Server 5.5, SP1-SP4**	**A Cross-Site Scripting vulnerability exists due to the way that Outlook Web Access (OWA) performs HTML encoding in the Compose New Message form, which could let a remote malicious user execute arbitrary code.** ***Removed unnecessary information from "Deployment" in the "Exchange Server 5.5 Service Pack 4" section of "Security Patch Information."***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-047.asp**	**Exchange Server 5.5 Outlook Web Access Cross-Site Scripting CVE Name: CAN-2003-0712**	**High**	**Bug discussed in newsgroups and websites.** ***Proof of Concept exploit script has been published.*** **Vulnerability has appeared in the press and other public media.**
Microsoft[75] ***Exploit script has been published & bulletin updated***[76, 77]	**Windows NT 4.0/2000**	**Exchange Server 5.5, SP1-SP4 Exchange 2000 Server, SP1-SP3**	**A buffer overflow vulnerability exists due to a failure to handle certain SMTP extended verbs correctly.** ***V1.1: Removed unnecessary information from "Deployment" in the "Exchange Server 5.5 Service Pack 4" section of "Security Patch information."***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-046.asp**	**Exchange Server Buffer Overflow CVE Name: CAN-2003-0714**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.*** **Vulnerability has appeared in the press and other public media.**

[69] Bugtraq, October 30, 2003.
[70] Mandrake Linux Security Update Advisory, MDKSA-2003:100, October 16, 2003.
[71] Conectiva Linux Security Announcement, CLA-2003:766, October 17, 2003.
[72] Slackware Security Bulletin, SA:2003-300-01, October 27, 2003.
[73] Microsoft Security Bulletin, MS03-047, October 15, 2003.
[74] Microsoft Security Bulletin, MS03-047 V1.1, October 22, 2003.
[75] Microsoft Security Bulletin, MS03-046, October 15, 2003.
[76] PacketStorm, October 29, 2003.
[77] Microsoft Security Bulletin, MS03-046 V 1.1, October 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[78] ***Microsoft updates bulletin***[79]	**Windows NT 4.0/2000**	**Exchange Server 5.5, SP1-SP4**	**A Cross-Site Scripting vulnerability exists due to the way that Outlook Web Access (OWA) performs HTML encoding in the Compose New Message form, which could let a remote malicious user execute arbitrary code.** **V1.1:** • **Removed unnecessary information from "Deployment" in the "Exchange Server 5.5 Service Pack 4" section of "Security Patch Information."** • **Updated product specific information in the "Exchange Server 5.5 Service Pack 4" section of "Security Patch Information."** • **Updated link in the "Severity Rating" section of "Technical Details."** **V2.0: Updated to include details of an additional patch for languages available through the Outlook Web Access language pack.**	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-047.asp**	**Exchange Server 5.5 Outlook Web Access Cross-Site Scripting** **CVE Name: CAN-2003-0712**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Microsoft[80]	Windows 98/MT/NT/ 2000, XP, 2003	HTML Help Control 5.2.3735.1	A vulnerability exists due to the HTML Help API not dropping privileges before invoking the help viewer, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Windows HTML Help API	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[81]	Windows	Internet Explorer 6.0 SP1	A vulnerability exists because restrictions can be bypassed when adding an additional slash when a resource is specified via 'file://' or 'res://' URLs, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Internet Explorer Local Resource Reference	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[78] Microsoft Security Bulletin, MS03-047, October 15, 2003.
[79] Microsoft Security Bulletin, MS03-047 V1.1 & V2.0, October 21 & 22, 2003.
[80] NTBugtraq, October 24, 2003.
[81] Bugtraq, October 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [82]	Windows 98/ME/NT 4.0/2000, 2003	Internet Explorer 6.0, SP1	A Denial of Service vulnerability exists due to improper handling of the scrollbar-base-color attribute of the div object.	No workaround or patch available at time of publishing.	Internet Explorer Scrollbar-Base-Color Partial Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [83] *Microsoft updates bulletin* [84]	**Windows NT 4.0/2000, 2003, XP**	**Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1**	**A buffer overflow vulnerability exists because the length of messages is not verified, which could let a remote malicious user execute arbitrary code.** ***V1.1: Updated the "Security Patch Information" section for Windows Server 2003, Windows XP, and Windows 2000.*** ***V2.0: A revised version of the security patch for Windows 2000, Windows XP, and Windows Server 2003 has been released to correct the issue documented by Knowledge Base Article 830846.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-043.asp**	**Messenger Service Buffer Overflow** **CVE Name: CAN-2003-0717**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.** ***Vulnerability has appeared in the press and other public media.***

[82] Bugtraq, October 22, 2003.
[83] Microsoft Security Bulletin, MS03-043, October 15, 2003.
[84] Microsoft Security Bulletin, MS03-043 V1.1 & V2.0, October 22 & 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [85] *Microsoft updates bulletin*[86]	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists because the 'ListBox' and 'ComboBox' controls due to insufficient validation of user-supplied parameters, which could let a remote malicious user execute arbitrary code. *V1.1: Re-issued to advise of a language specific compatibility issue with some third-party software.* *V2.0 : Version changed to reflect the availability of updated patch for specific languages.* *V3.0: A revised version of the security patch for Windows XP has been released to correct the issue documented by Knowledge Base Article 830846.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-045.asp	Windows ListBox & ComboBox Control Buffer Overflow CVE Name: CAN-2003-0659	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[85] Microsoft Security Bulletin MS03-045, October 15, 2003.
[86] Microsoft Security Bulletin MS03-045 V1.1, V2.0 & V3.0, October 17, 22, & 29, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [87] *Microsoft updates bulletin*[88]	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A vulnerability exists in 'Authenticode' because under certain low memory conditions an ActiveX control can be downloaded and installed without presenting the user with an approval dialog, which could let a remote malicious user execute arbitrary code. *Updated "File Information" in the "Windows 2000" section of "Security Patch Information."*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-041.asp	Microsoft ActiveX Authenticode Verification Bypass CVE Name: CAN-2003-0660	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[87] Microsoft Security Bulletin, MS03-041, October 15, 2003.
[88] Microsoft Security Bulletin, MS03-041 V1.1, October 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [89] *Microsoft updates bulletin* [90]	Windows NT 4.0/2000, XP, 2003	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Profes-sional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Work-station 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Profes-sional, SP1	A buffer overflow vulnerability exists in the URI Handler in the Help and Support Center (HSC) due to insufficient bounds checking when handling 'hcp://' URI links, which could let a remote malicious user execute arbitrary code. *Updated download link for Windows XP 64 bit edition Version 2003.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-044.asp	Windows Help And Support Center URI Handler Remote Buffer Overflow CVE Name: CAN-2003-0711	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[89] Microsoft Security Bulletin MS03-044, October 15, 2003.
[90] Microsoft Security Bulletin MS03-044 V1.1, October 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[91] ***Microsoft updates bulletin***[92]	**Windows 2000**	**Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Profes-sional, SP1-SP4, 2000 Server, SP1-SP4**	**A buffer overflow vulnerability exists in the TroubleShooter ActiveX control, which could let a remote malicious user execute arbitrary code.** ***V1.1: Updated product specific information in the Security Patch Information section.*** ***V2.0: A revised version of the security patch for Windows 2000 has been released to correct the issue documented by Knowledge Base Article 830846.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-042.asp**	**Windows 2000 Trouble Shooter ActiveX Control Buffer Overflow** **CVE Name: CAN-2003-0662**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.** **Vulnerability has appeared in the press and other public media.**
mod_ security[93]	Unix	mod_ security 1.7, 1.7.1	A buffer overflow vulnerability exists when handling large amounts of data transferred via server-side scripts due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.modsecurity.org/download/mod_security-1.7.2.tar.gz	Mod_Security Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[94]	Unix	Dug Song dsniff 2.3; Rafal Wojtczuk Libnids 1.11-1.14, 1.16, 1.17	A buffer overflow vulnerability exists due to a memory corruption flaw that can be triggered by excessive size TCP packets, which could let a remote malicious user execute arbitrary code.	Update available at: http://prdownloads.sourceforge.net/libnids/libnids-1.18.tar.gz?download **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Rafal Wojtczuk:** https://sourceforge.net/project/showfiles.php?group_id=92215	Libnids TCP Packet Reassemble Remote Buffer Overflow CVE Name: CAN-2003-0850	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[95, 96]	Unix	GNU fileutils 4.0, 4.0.36, 4.1, 4.1.6, 4.17; Washing-ton University wu-ftpd 2.4.1, 2.4.2 academ BETA1-15, BETA-18, 2.4.2 VR10 -VR17, 2.5.0, 2.6.0-2.6.2	An integer overflow vulnerability exists in /bin/ls, which could let a remote malicious user cause a Denial of Service.	Patches available at: http://mail.gnu.org/archive/html/bug-coreutils/2003-10/msg00070.html **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Coreutils LS Width Argument Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit script has been published.

[91] Microsoft Security Bulletin, MS03-042, October 15, 2003.
[92] Microsoft Security Bulletin, MS03-042 V1.1 & V2.0, October 21 & 29, 2003.
[93] Bugtraq, October 28, 2003.
[94] Conectiva Linux Security Announcement, CLA-2003:773, October 29, 2003.
[95] Georgi Guninski Security Advisory #62, October 22, 2003
[96] Conectiva Linux Security Announcement, CLA-2003:768 & CLA-2003:771, October 22 & 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [97, 98] *VMWare issues upgrade*[99]	Unix	OpenSSL Project OpenSSL 0.9.6-0.9.6e; EnGarde Secure Community 1.0.1, Secure Profes-sional 1.1, 1.2; Red Hat Linux 7.1, 7.1 for iSeries, 7.1 for pSeries, 7.2, 7.3, 8.0	A remote Denial of Service vulnerability exists when processing a specially crafted malicious CLIENT_MASTER_KEY message.	**OpenSSL Project:** http://www.openssl.org/source/ **EnGarde:** http://www.linuxsecurity.com/advisories/engarde_advisory-3709.html **RedHat:** ftp://updates.redhat.com/ ***VMWare:*** http://www.vmware.com/download/gsx_security.html http://www.vmware.com/download/esx/esx2-openssh.html	OpenSSL SSLv2 Client_Master_Key Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Multiple Vendors [100, 101, 102, 103] *Conectiva issues advisory* [104] *SGI issues advisory* [105]	Unix	pam_smb 1.1-1.1.6, 2.0 -rc4,; RedHat pam_smb-1.1.6-2.i386.rpm, 1.1.6-2.ia64.rpm, 1.1.6-5.i386.rpm, 1.1.6-7.i386.rpm	A buffer overflow vulnerability exists due to a boundary error when handling passwords, which could let a remote malicious user execute arbitrary code with root privileges.	**Debian:** http://security.debian.org/pool/updates/main/libp/libpam-smb/ **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **TurboLinux:** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/ **SGI:** http://www.sgi.com/support/security/	Pam_SMB Remote Buffer Overflow CVE Name: CAN-2003-0686	High	Bug discussed in newsgroups and websites. Exploit script has been published.

[97] RedHat Security Advisory, RHSA-2003:291-11, September 30, 2003.
[98] Guardian Digital Security Advisory, ESA-20031003-028, October 3, 2003.
[99] SecurityFocus, October 29, 2003.
[100] Debian Security Advisory, DSA 374-1, August 26, 2003.
[101] Red Hat Security Advisories, RHSA-2003:261-01 & RHSA-2003:262-07, August 26, 2003.
[102] Turbo Linux Security Announcement, TLSA-2003-50, August 29, 2003.
[103] SuSE Security Announcement, SuSE-SA:2003:036, September 3, 2003.
[104] Conectiva Linux Security Announcement, CLA-2003:734, September 5, 2003.
[105] SGI Security Advisory, 20031002-01-U, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [106, 107, 108] *SGI issues advisory* [109]	Unix	Martin K. Peterson gdm 2.2.0, 2.2.2.1, 2.2.5 4, 2.4.1, 2.4.1.1-2.4.1.6; RedHat Enterprise Linux WS 2.1 IA64, 2.1, Linux ES 2.1 IA64, 2.1, Linux AS 2.1 IA64, 2.1, gdm-2.0beta2-45.i386.rpm, ppc.rpm, 2.0beta2-45.ppc.rpm, 2.2.3.1-20.i386.rpm, 20.ia64.rpm, gdm-2.2.3.1-22.i386.rpm, gdm-2.4.0.7-13.i386.rpm, gdm-2.4.1.3-5.i386.rpm Linux Advanced Work Station 2.1	Multiple remote Denial of Service vulnerabilities exist when X Display Manager Control XDMCP is running in conjunction with GDM.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/advisories/ RedHat: ftp://updates.redhat.com/ SGI: ftp://patches.sgi.com/support/free/security/	Multiple XDMCP GDM Multiple Remote Denial of Service Vulnerabilities CVE Names: CAN-2003-0548, CAN-2003-0549	Low	Bug discussed in newsgroups and websites.

[106] Mandrake Linux Security Update Advisory, MDKSA-2003:085, August 21, 2003.
[107] Red Hat Security Advisories, RHSA-2003:258-01 & RHSA-2003:259-07, August 21, 2003.
[108] Conectiva Linux Security Announcement, CLA-2003:729, August 29, 2003.
[109] SGI Security Advisory, 20031002-01-U, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB[110, 111, 112] *More advisories issued*[113, 114, 115, 116] *More advisories issued*[117, 118, 119] *SGI issues advisory*[120]	Unix	MySQL 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.56, 4.0.0-4.0.14. 4.1.0-alpha, 4.1 .0-0	A buffer overflow vulnerability exists when handling user passwords of excessive size due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Patch available at: http://www.mysql.com/downloads/mysql-4.0.html **Debian:** http://security.debian.org/pool/updates/main/m/mysql/ **OpenPKG:** Ftp://ftp.openpkg.org/release/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/ ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/ ***Engarde:*** http://www.linuxsecurity.com/advisories/engarde_advisory-3650.html ***Mandrake:*** http://www.mandrakesecure.net/en/ftp.php ***SuSE:*** ftp://ftp.suse.com/pub/suse ***RedHat:*** Ftp://updates.redhat.com/ ***TurboLinux:*** ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ ***SGI:*** http://www.sgi.com/support/security/	MySQL Password Handler Buffer Overflow CVE Name: CAN-2003-0780	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. An exploit script has also been published.

[110] Debian Security Advisory, DSA 381-1, September 14, 2003.
[111] OpenPKG Security Advisory, OpenPKG-SA-2003.038, September 15, 2003.
[112] Trustix Secure Linux Security Advisory, TSLSA-2003-09-17, September 17, 2003.
[113] Conectiva Linux Security Announcement, CLA-2003:743, September 18, 2003.
[114] Guardian Digital Security Advisory, ESA-20030918-025, September 18, 2003.
[115] Mandrake Linux Security Update Advisory, MDKSA-2003:094, September 18, 2003.
[116] SuSE Security Announcement, SuSE-SA:2003:042, October 1, 2003
[117] TurboLinux Security Advisory, TLSA-2003-56, October 7, 2003.
[118] Red Hat Security Advisory, RHSA-2003:281-01, October 9, 2003.
[119] Conectiva Linux Security Announcement, CLSA-2003:764, October 16, 2003.
[120] SGI Security Advisory, 0031002-01-U, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nicolas Boullis[121] ***Exploit script published***[122] ***Another exploit script published***[123]	**Unix**	**Mah-Jong 1.4**	**Several vulnerabilities exist: a buffer overflow vulnerability exists when a specially crafted command is submitted to the server, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists due to the way escaped characters are processed.**	**Debian:** **http://security.debian.org/pool/updates/main/m/mah-jong/**	**Mah-Jong Server Remote Buffer Overflow & Denial of Service** **CVE Names: CAN-2003-0705, CAN-2003-0706**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Nokia[124]	Multiple	IPSO 3.1.3, 3.3 SP1-SP4, 3.3.1, 3.4, 3.4.1, 3.4.2, 3.5-3.7	A remote Denial of Service vulnerability exists when the system has been configured with IP Clustering.	Update available at: https://support.nokia.com/security_platforms/index.jsp	Nokia IPSO Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Novell[125] ***Support Pack 2 beta now available***[126]	**Multiple**	**iChain Server 2.2, FP1a, FP1**	**A vulnerability exists when a new user's session is opened on the same port as another user's session, which could let a malicious user inherit another user's session.**	**Upgrade available at: http://support.novell.com/servlet/filedownload/sec/ftf/ic22fp2.exe** ***Upgrade available at:*** **http://support.novell.com/servlet/filedownload/sec/ftf/b2ic22sp2.exe**	**iChain Session Inheritance**	**Medium**	**Bug discussed in newsgroups and websites.**
Novell[127]	Multiple	Netware 6.0 SP3, ZENworks for Desktops 3.2 SP2, 4.0, 4.0.1	A buffer overflow vulnerability exists in the 'PMAP.NLM' component, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Novell 'PMAP.NLM' Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[121] Debian Security Advisory, DSA 378-1, September 7, 2003.
[122] SecurityFocus, October 16, 2003.
[123] SecurityFocus, October 22, 2003.
[124] Secunia Advisory, SA10083, October 29, 2003.
[125] Novell Technical Information Document, TID2966683, August 8, 2003.
[126] Technical Information Document, TID2967231, October 23, 2003.
[127] Novell Technical Information Document, TID10088194, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell[128] ***Upgrade now available***[129]	**Multiple**	**iChain Server 2.2, SP1, FP1a, FP1**	**A Denial of Service vulnerability exists when a retrieve request is submitted by 'wget' on a directory that has no files.**	**Workaround:** **Create a dummy file (small text file) in each of the following directories:** **sys:\etc\proxy\appliance\config\user\cert\backup** **sys:\etc\proxy\appliance\config\user\cert\temp** **sys:\etc\proxy\appliance\config\user\cert\ics** **sys:\etc\proxy\appliance\config\user\cert\sc** **sys:\etc\proxy\appliance\config\user\cert\tr** ***Upgrade available at:*** **http://support.novell.com/servlet/filedownload/sec/ftf/b2ic22sp2.exe**	**iChain Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
Opera Software[130]	Windows, Unix	Opera Web Browser 7.11, 7.20	A buffer overflow vulnerability exists when handling malformed HTML HREF values, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.opera.com/download/	Opera HREF Malformed Buffer Overflow CVE Name: CAN-2003-0870	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Oracle Corporation[131]	Unix	Oracle9i Enterprise Edition 9.0.1, 9.2.0.4, Oracle9i Personal Edition 9.0.1, 9.2.0.4, Oracle9i Standard Edition 9.0, 9.0.1.4, 9.0.1.3. 9.0.1.2, 9.0.1, 9.0.2, 9.2 .0.4	Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'oracle' binary due to insufficient bounds checks performed on command line arguments, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'OracleO' binary due to a lack of sufficient bounds checking performed on command line arguments passed to the affected binary, which could let a malicious user execute arbitrary code.	A one-off patch has been released to address this issue in Oracle 9i Database Release 9.2.0.4 for Linux x86 and can be obtained from the following URL: http://metalink.oracle.com/	Oracle Database Server Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Proof of Concept script has been published for the 'oracle' binary vulnerability.

[128] Novell Technical Document, 10086051, August 20, 2003
[129] Technical Information Document, TID2967231, October 23, 2003.
[130] @stake, Inc. Security Advisory, A102003-1, October 20, 2003.
[131] Oracle Security Alert 59, October 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation[132]	Windows NT 4.0/2000, Unix	Oracle Files 9.0.3.1.0-9.0.3.3.0	A vulnerability exists in Oracle Files, a component of Oracle Collaboration Suite Release 1, which could let a remote malicious user obtain access to restricted files.	Updates are available at: http://metalink.oracle.com/	Oracle Files Restricted Content Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
ORIGO Inc.[133]	Multiple	ASR-8100 ADSL Router 3.21, ASR-8400 ADSL Router	An authentication vulnerability exists due to insufficient access controls, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Origo ADSL Router Remote Administrative Interface Configuration	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Paul Smith Computer Services [134]	Windows	VPOP3 2.0f, 2.0 e	A Cross-Site Scripting vulnerability exists in the WebAdmin utility due to insufficient filtering of HTML code from user-supplied input, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.pscs.co.uk/downloads/vpop3.html	VPOP3 WebAdmin Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PGPi[135]	Windows	PGPDisk 6.0.2i	An information disclosure vulnerability exists in the 'switch user' function, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	PGPDisk Switched User Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
phpinfo.net [136]	Windows, Unix	Les Visiteurs 2.0, 2.0.1	A vulnerability exists in the 'include/config.inc.php' and 'include/new-visitor.inc.php' files due to insufficient validation, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Les Visiteurs Remote File Include Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Postgre SQL[137] ***Vendors issue advisories*** *138, 139*	**Unix**	**Postgre SQL 7.2-7.2.4, 7.3-7.3.3**	**A buffer overflow vulnerability exists in the 'PostgreSQL to_ascii()' function, which could let a malicious user execute arbitrary code.**	**Upgrade available at: http://www.postgresql.org/** ***Conectiva:*** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000772** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/1.2/UPD/**	**PostgreSQL To_Ascii() Buffer Overflow** **CVE Name: CAN-2003-0901**	**High**	**Bug discussed in newsgroups and websites.**

[132] Oracle Security Alert #60, October 28, 2003.
[133] SecurityTracker Alert, 1007965, October 20, 2003.
[134] Securiteam, October 20, 2003.
[135] Securiteam, October 22, 2003.
[136] Secunia Advisory, SA10079, October 28, 2003.
[137] SecurityFocus, October 1, 2003.
[138] Conectiva Linux Announcement, CLSA-2003:772, October 24, 2003.
[139] OpenPKG Security Advisory, OpenPKG-SA-2003.047, October 30, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Proxy2.de [140]	Windows, Unix	Advanced Poll 2.0.2	Multiple vulnerabilities exist: a vulnerability exists in the 'id,' 'template_set,' and 'action' parameters due to insufficient verification before being used in an 'eval()' function call, which could let a remote malicious user execute arbitrary PHP code; a vulnerability exists in the 'booth.php,' 'png.php,' 'poll_ssi.php,' and 'popup.php' scripts due to a failure to verify the 'include_path' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'admin/common.inc.php' file due to a failure to verify the 'base_path' parameter, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'misc/info.php' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple Advanced Poll PHP Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerabilities may be exploited via a web browser. Exploit has been published.
RedHat [141]	Unix	httpd-2.0.40-21.5.i386.rpm	A vulnerability exists in the RedHat Apache configuration when a 'HTTP GET' request is issued that contains certain characters, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	RedHat Apache Directory Index Default Configuration	Medium	Bug discussed in newsgroups and websites.

[140] Bugtraq, October 25, 2003.
[141] Bugtraq, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Rit Research Labs[142]	Windows 95/98/ME/ NT 4.0/2000, XP	The Bat! 1.043, 1.041, 1.039, 1.035-1.037, 1.032, 1.031, 1.029, 1.028, 1.015, 1.011, 1.1, 1.5, 1.14, 1.15, 1.17-1.19, 1.21, 1.22, 1.31-1.36, 1.39, 1.41-1.49, 1.51, 1.52, 1.53 d, 1.101, 2.01, 2.0	A vulnerability exists because new accounts are created with unsafe permissions in the '%programfiledir%\The Bat!\MAIL\' directory, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	The Bat! Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[142] SecurityTracker Alert, 1008004, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SANE[143] ***More advisories issued***[144, 145] ***More advisories issues***[146] [147]	**Unix**	**SANE 1.0.0-1.0.9, sane-backend 1.0.10**	**Multiple vulnerabilities exist: a vulnerability exists because the identity (IP address) of the remote host is not checked during the SANE_NET_INIT RPC call, which could let a remote malicious user obtain unauthorized access; a vulnerability exists because connection drops are not handled properly, which could let a remote malicious user obtain sensitive information and cause a Denial of Service; a vulnerability exits when a connection is dropped before the size value of malloc is set, which could let a remote malicious user cause a Denial of Service; a vulnerability exists because the validly of RPC numbers it gets before getting the parameters; a vulnerability exists when debug messages are enabled dropped connections are not properly handled, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists because memory is not properly allocated in some cases, which could let a remote malicious user cause a Denial of Service.**	**Debian:** **Http://security.debian.org/pool/updates/main/s/sane-backends/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **SGI:** **http://www.sgi.com/support/security/**	**Multiple Sane Package Remote Vulnerabilities** **CVE Names: CAN-2003-0773, CAN-2003-0774, CAN-2003-0775, CAN-2003-0776, CAN-2003-0777, CAN-2003-0778**	**Low/ Medium** **(Medium if unauthorized access or sensitive information can be obtained)**	**Bug discussed in newsgroups and websites.**
SCO[148]	Unix	Open Server 5.0.5	Vulnerabilities exist because several scripts use /tmp files in a insecure way, which could let a malicious user obtain elevated privileges.	Updates available at: ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.27/VOL.000.000	OpenServer Insecure Temporary File Vulnerabilities CVE Name: CAN-2003-0872	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[143] Debian Security Advisory DSA 379-1, September 11, 2003.
[144] Red Hat Security Advisories, RHSA-2003:278-01 & RHSA-2003:285-03, October 7, 2003.
[145] Mandrake Linux Security Update Advisory, MDKSA-2003:099, October 10, 2003.
[146] Conectiva Linux Security Announcement, CLA-2003:769, October 22, 2003.
[147] SGI Security Advisory, 20031002-01-U, October 27, 2003.
[148] SCO Security Advisory. CSSA-2003-SCO.27, October 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI[149]	Unix	RIX 6.5.21m, 6.5.21 f	A vulnerability exists when any of the root, rw, or access options in the '/etc/exports' file contains a wildcard with no hostnames or netgroups, which could let a remote malicious user obtain unauthorized access.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/6.5.21	IRIX Wildcard Entry Unauthorized Access CVE Name: CAN-2003-0683	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[150]	Windows, Unix	Java SDK 1.4.x, 1.3.x, 1.2.x, JRE 1.4.x, 1.3.x, 1.2.x	A vulnerability exists when implementing the Security Manager, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Java Virtual Machine Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Micro-systems, Inc.[151]	Windows	Java Plug-In 1.4, 1.4.2_02, 1.4.2_01	A vulnerability exists in the Java security model, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Sun Java Unauthorized Access	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Micro-systems, Inc.[152]	Windows, Unix	Java Plug-In 1.4.2 _01	A vulnerability exists because certain undocumented static variables are accessible from shared memory by different applets at the same time, which could let a malicious user bypass security restrictions, manipulate data, or obtain sensitive information. This has been reported to affect the 'org.apache.xalan.processor.XSLProcessorVersion' class.	No workaround or patch available at time of publishing.	Sun Java Cross-Site Applet Sandbox Security Model Violation	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Micro-systems, Inc.[153]	Windows, Unix	SDK & JRE 1.4.1_03 & prior, SDK & JRE 1.3.1_08 & prior, SDK & JRE 1.2.2_015 & prior	A vulnerability exists due to a logic flaw in the implementation of the 'loadClass' method of the 'sun.applet.AppletClassLoader' class, which could let a local/remote malicious user circumvent the Java Security Model and execute arbitrary code.	Updates available at: http://java.sun.com/j2se/	Sun Java Virtual Machine Slash Path Security Model Circumvention	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[149] SGI Security Advisory, 20031004-01-P, October 28, 2003.
[150] SecurityFocus, October 27, 2003.
[151] Bugtraq, October 21, 2003.
[152] Bugtraq, October 20, 2003.
[153] Sun(sm) Alert Notification, 57221, October 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[154] ***Exploit script has been published***[155]	**Unix**	**Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86**	**A buffer overflow vulnerability exists in the ld runtime linker due to insufficient bounds checking performed in the routines used to process the value of LD_PRELOAD, which could let a malicious user execute arbitrary code with root privileges.**	**Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/55680**	**Solaris Runtime Linker Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.** ***Exploit script has been published.***
Sun Micro-systems, Inc.[156]	Unix	Solaris 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A remote Denial of Service vulnerability exists when a Solaris NFS Server receives certain invalid requests from a client for a shared UFS file system	Patches available at: http://sunsolve.sun.com	Solaris NFS Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[157]	Unix	Solstice X.25 9.1, 9.2	Two vulnerabilities exist: a remote Denial of Service vulnerability exists due to improper handling of exceptional conditions by the 'snmpx25d' daemon; and a buffer overflow vulnerability exists in the 'snmpx25d' daemon due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Workaround and patch information available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57404	Solstice Remote Denial of Service & Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[158]	Unix	SunMC 2.1.1, 3.0, 3.5	A vulnerability exists due to the way error messages are handled, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Sun Management Center Error Message Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Symantec[159]	Windows	Norton Internet Security 2003 6.0.4 .34	A Cross-Site Scripting vulnerability exists due to missing input validation when a requested URL is included in a blocked site error message returned to the user, which could let a remote malicious user execute arbitrary HTML or script code.	Symantec has released a fix to address this issue. Users are advised to download the patch through the LiveUpdate feature of the software.	Norton Internet Security Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[154] iDEFENSE Security Advisory, July 29, 2003.
[155] SecurityFocus, October 27, 2003.
[156] Sun(sm) Alert Notification, 57406, October 27, 2003.
[157] Sun(sm) Alert Notification, 57404, October 22, 2003.
[158] SecurityFocus, October 22, 2003.
[159] DigitalPranksters Security Advisory, October 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Tel-Condex Software [160]	Windows	SimpleWeb Server 2.12.30210 build 3285	A buffer overflow vulnerability exits due to a boundary error when handling the 'Referer:' header, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.yourinfosystem.de/download/TcSimpleWebServer2000Setup.exe	Simple Webserver HTTP Referer Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
University of Washington [161, 162, 163, 164, 165] ***Turbo Linux issues advisory [166]*** ***SGI issues advisory [167]***	**Unix**	**Pine 3.98, 4.0.2, 4.0.4, 4.10, 4.20, 4.21, 4.30, 4.33, 4.44, 4.50, 4.52, 4.543, 4.56**	**Two vulnerabilities exist: a buffer overflow vulnerability exists when handling 'message/external body type' attributes due to a boundary error, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the 'rfc2231_get_param()' function when parsing e-mail headers, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at: http://www.washington.edu/pine/getpine/ Conectiva: ftp://atualizacoes.conectiva.com.br/7 Engarde: http://infocenter.guardiandigital.com/advisories/ RedHat: ftp://updates.redhat.com/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SuSE: ftp://ftp.suse.com/pub/suse *TurboLinux:* ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ SGI: http://www.sgi.com/support/security/**	**Pine Buffer Overflow & Integer Overflow CVE Names: CAN-2003-0720, CAN-2003-0721**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published for the buffer overflow vulnerability.**
Vivisimo, Inc. [168]	Windows, Unix	Clustering Engine	A Cross-Site Scripting vulnerability exists in the 'query' parameter due to insufficient validation of user-supplied input when processing search queries, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Vivisimo Clustering Engine Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Washington University [169]	Unix	wu-ftpd 2.6.0-2.6.2	A buffer overflow vulnerability exists if support for 'S/Key' authentication is enabled due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Wu-Ftpd S/Key Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[160] Bugtraq, October 29, 2003.
[161] Slackware Security Advisory, SSA:2003-253-01, September 10, 2003.
[162] SuSE Security Announcement, SuSE-SA:2003:037, September 10, 2003.
[163] Guardian Digital Security Advisory, ESA-20030911-022 , September 11, 2003
[164] Red Hat Security Advisory, RHSA-2003:273-01, September 11, 2003.
[165] Conectiva Linux Security Announcement, CLA-2003:738, September 12, 2003.
[166] TurboLinux Security Advisory, TLSA-2003-57, October 8, 2003.
[167] SGI Security Advisory, 20031002-01-U, October 27, 2003.
[168] SecurityTracker Alert, 1007955, October 18, 2003.
[169] Secunia Advisory, SA10077, October 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Web Wiz Guide[170]	Windows	Web Wiz Forums 7.01	Cross-Site Scripting vulnerabilities exist in the 'members.asp,' and 'pm_buddy_list.asp' scripts due to insufficient filtering, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Wiz Forums Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Wireless Tools For Linux[171]	Unix	Wireless Tools Versions 19-26	A buffer overflow vulnerability exists in the 'iwconfig' program when handling strings on the commandline, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	IWConfig Command Line Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Yahoo![172]	Windows	Messenger 5.6	A buffer overflow vulnerability exists due to a boundary error in the file transfer functionality ("ft.dll"), which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Yahoo! Messenger File Transfer Remote Buffer Overrun	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between October 17 and October 31, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 26 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

[170] Bugtraq, October 22, 2003.
[171] Securiteam, October 26, 2003.
[172] SecurityTracker Alert, 1008008, October 27, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
October 31, 2003	vote.pdf 244831	This paper describes several security flaws in Diebold electronic voting machines. Voters may be able to cast multiple ballots with little built in traceability, administrative functions can be performed by regular voters, and inside poll workers, software developers, and janitors can rig the vote. The smart card system is insecure and uses plaintext passwords. The code appears unaudited and there is no ability to do a paper recount.
October 30, 2003	telecondex.pl	Perl script that exploits TelCondex Remote Denial of Service Buffer Overflow vulnerability.
October 30, 2003	**x-ws_ftp.c**	**Script that exploits the WS_FTP Server Buffer Overflow vulnerability.**
October 29, 2003	**cpCommerce.exp.txt**	**Exploit URL for the CPCommerce Functions Remote Code Execution vulnerability.**
October 29, 2003	ebpoverflow.txt	A paper that describes how to exploit overflows which are off by only one byte.
October 29, 2003	hydra-2.4.tar.gz	A high quality parallized login hacker for Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more.
October 29, 2003	iweb.traversal.txt	Exploit URLs for the iWeb Mini HTTP Server Directory Traversal vulnerability.
October 29, 2003	**kpopup-exp.c**	**Script that exploit the kpopup Privileged Command Execution vulnerability.**
October 29, 2003	ld.so.exp.c	Script that exploits the Solaris Runtime Linker Buffer Overflow vulnerability.
October 29, 2003	ls_ftp.pl	Perl script that exploits the Coreutils LS Width Argument Remote Denial of Service vulnerability.
October 29, 2003	ms03-046.pl	Perl script that exploits the Exchange Server 5.5 Outlook Web Access Cross-Site Scripting vulnerability.
October 29, 2003	**php.advanced.poll.txt**	**Exploit URLs and vulnerable code snippets for the Advanced Poll PHP Vulnerabilities.**
October 29, 2003	thcrut-1.2.5.tar.gz	A local network discovery tool developed to brute force its way into wvlan access points that offers arp-request on ip-ranges and identifies the vendor of the NIC, spoofed DHCP, BOOTP and RARP requests, icmp-address mask request and router discovery techniques.
October 29, 2003	yax-phpnuke.sh	Exploit for the PHP-Nuke v6.6 and spaiz-nuke below v1.2beta Administrative Account vulnerability.
October 27, 2003	**0x82-Local.musicqueue_xpl.c**	**Script that exploits the Musicqueue SIGSEGV Signal Handler Insecure File Creation vulnerability.**
October 27, 2003	**0x82-musicqueue_over.c**	**Script that exploits the Musicqueue Multiple Buffer Overflows vulnerabilities.**
October 27, 2003	asl_plz.txt	Exploit for the mIRC DCC SEND Variant Buffer Overflow vulnerability.
October 27, 2003	btscanner-1.0.tar.gz	A tool which extracts as much information as possible from a Bluetooth device.
October 26, 2003	**PST_iwconfig.c**	**Script that exploits the IWConfig Command Line Buffer Overflow vulnerability.**
October 22, 2003	xmjong.c	Script that exploits the Mah-Jong Server Remote Buffer Overflow & Denial of Service vulnerability.
October 21, 2003	winsyslog-DoS.pl	Perl script that exploits the WinSyslog Interactive Syslog Server Long Message Remote Denial of Service vulnerability.
October 20, 2003	gEEk-fuck-khaled.c	Script that exploits the mIRC IRC URL Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
October 20, 2003	ngrep-1.41.tar.bz2	A powerful network sniffing tool which strives to provide most of GNU grep's common features, applying them to all network traffic. It is a pcap-aware tool that will allow you to specify extended regular expressions to match against data payloads of packets.
October 20, 2003	redfang.2.5.tar.gz	An enhanced version of the original application that finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the device's Bluetooth address and doing a read_remote_name().
October 17, 2003	libShellCode-0.2.1.tar.gz	A library that can be included when writing linux/i386 exploits by providing functions that generate shellcode with user given parameters during runtime.
October 17, 2003	oracle_ownage.c	Script that exploits the Oracle Database Server Buffer Overflows vulnerability.

Trends

- **The SANS Twenty Most Critical Internet Security Vulnerabilities list has been published. This updated SANS Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux. For more information see the list located at: http://www.sans.org/top20/.**
- **The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting the Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS) vulnerability. For more information, see "Bugs, Holes & Patches" Table and advisory located at: http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm. The Microsoft advisory is located at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp. Tools have been developed to exploit this vulnerability and there is an increased likelihood that new viruses will emerge soon.**
- **The CERT/CC has noticed an increase in traffic directed at port 554/tcp. This port is used by the Real Time Streaming Protocol (RTSP). This activity may be related to a recently discovered vulnerability in Real Networks' Media Server. For more information see" Helix Universal Server Remote Buffer Overflow" entry in the "Bugs, Holes & Patches" Table.**
- **Online vandals are using a program to compromise Windows servers and remotely control them through Internet relay chat (IRC) networks. Several programs, including one that exploits a recent vulnerability in computers running Windows, have been cobbled together to create a remote attack tool. The tool takes commands from a malicious user through the IRC networks and can scan for and compromise computers vulnerable to the recently discovered flaw in Windows The CERT/CC has received reports of systems being compromised by two recently discovered vulnerabilities in the Microsoft Remote Procedure Call (RPC) service. Additionally, the CERT/CC has received reports of widespread scanning for systems with open Microsoft RPC ports (135, 139, 445). For more information, see "Exploitation of Microsoft RPC Vulnerabilities" located at: http://www.cert.org/current/.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

W32/Agobot-AA (Alias: Backdoor.Agobot.3.h) (Win32 Worm): This worm has been reported in the wild. It is capable of spreading to computers on the local network protected by weak passwords. The worm copies itself to the Windows System folder as Lsas.exe and creates the following registry entries, so that Lsas.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows Explorer= LSAS.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Windows Explorer= LSAS.exe

Each time W32/Agobot-AA is run, the worm attempts to connect to a remote IRC server and join a specific channel. It then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels.

W32/Agobot-AF (Alias: W32/Gaobot.worm.gen) (Win32 Worm): This worm has been reported in the wild. It copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks please see Microsoft security bulletins MS03-026 and MS03-001. W32/Agobot-AF copies itself to the Windows system folder as SCVHOST.EXE and creates the following entries in the registry to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Config Loader = SCVHOST.EXE
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Config Loader = SCVHOST.EXE

W32/Agobot-AF attempts to terminate various processes related to anti-virus and security software (e.g. SWEEP95.EXE, BLACKICE.EXE and ZONEALARM.EXE).

W32.Cesca (Win32 Virus): This is a virus designed to spread through floppy disks. It periodically copies itself to the floppy using the file names that are randomly chosen from a list that the virus carries. It is written in the Microsoft programming language.

W32/Dafly-B (Aliases: Win32/Dafly.B, Worm.P2P.Dafly.b, W32/Dafly.worm) (Win32 Worm): This is a prepending virus that infects Windows executable files. It copies itself to the Windows system folder with the filenames SysDrv32.exe and Enjoy.exe and then sets the following registry entries to point to itself so that it is executed every time one of those filetypes is run (though a bug means that it may crash):

- HKCR\batfile\shell\open\command\
- HKCR\comfile\shell\open\command\
- HKCR\exefile\shell\open\command\
- HKCR\piffile\shell\open\command\
- HKCR\scrfile\shell\open\command\

W32/Dafly-B infects all files in the folder and subfolders pointed to by the following registry entries:

- HKCU\Software\Widcomm\BTConfig\Services\0005\root
- HKLM\Software\Kazaa\CloudLoad\ShareDir

It will also copy itself to the folders pointed to by these entries with the filenames Matrix2.scr and Terminator3.scr. W32/Dafly-B keeps a track of how many files it has infected by setting the number in the registry entry HKLM\Software\Microsoft\Windows\CurrentVersion\Infected. After infecting 49 files, W32/Dafly-B will delete files instead of infecting them. W32/Dafly-B tries to stop registry tools from being run by setting the following key:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools = "1"

W32/Dafly-B tries to read the key value HKCU\Identies\Default User ID. The virus then tries to set the following entries:

- HKCU\Identities\<Default User ID>\Software\Microsoft\Outlook Express\5.0\Signature Flags = "1"
- HKCU\Identities\<Default User ID>\Software\Microsoft\Outlook Express\5.0\Signatures\Default Signature = "00000000"
- HKCU\Identities\<Default User ID>\Software\Microsoft\Outlook Express\5.0\Signatures\00000000\file = "<Windows system>\Enjoy.exe"
- HKCU\Identities\<Default User ID>\Software\Microsoft\Outlook Express\5.0\Signatures\00000000\name = "MADFYLY"
- HKCU\Identities\<Default User ID>\Software\Microsoft\Outlook Express\5.0\Signatures\00000000\text = ""
- HKCU\Identities\<Default User ID>\Software\Microsoft\Outlook Express\5.0\Signatures\00000000\type = "2"

W32/Dafly-B checks for the presence of the registry entry, HKLM\Software\IDAVLab\DRWEB32W\ExePath. If this registry entry exists, then the virus will not infect files that are run from the folder that it references, but will instead display the message "Dr.Web for Windows 95-XP. EVALUATION version! To get your registration key, call regional dealer." W32/Dafly-B will then also try to delete a registry entry from HKCR\CLSID. W32/Dafly-B sets the following registry entry in the course of execution:

- HKCU\Software\Microsoft\Internet Explorer\Main\Start Page = "MADFLY.TK"

W32/Donk-E (Aliases: W32/Sdbot.worm, W32.HLLW.Donk.B, BKDR_SDBOT.Y) (Win32 Worm): This is a network worm and backdoor Trojan that copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC vulnerability. This vulnerability allows the worm to execute its code on target computers with System level privileges. For further information on this vulnerability and for details on how to protect/patch the computer, see Microsoft security bulletin MS03-026. When first run, W32/Donk-E copies itself to the Windows system folder as COOL.EXE and NETAPI32.EXE and creates the following registry entries so that NETAPI32.EXE is run automatically each time Windows is started:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Microsoft System Checkup = netapi32.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft System Checkup = netapi32.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\NT Logging Service = syslog32.exe

W32/Donk-E fails to copy itself as syslog32.exe. It connects to other computers on the local network. If a computer has a weak password, W32/Donk-E copies itself to the following startup folders:

- \WINNT\Profiles\All Users\Start Menu\Programs\Startup
- \WINDOWS\Start Menu\Programs\Startup
- \Documents and Settings\All Users\Start Menu\Programs\Startup

It also includes backdoor Trojan functionality that allows a remote intruder to access and control the computer via IRC channels. Each time W32/Donk-E is run, it tries to connect to a remote IRC server and join a specific channel. W32/Donk-E then runs continuously in the background as a service process listening for commands to execute.

W32.HLLW.Franriv (Alias: WORM_FRANRIV.A) (Win32 Worm): This is a worm that attempts to spread through the KaZaA file-sharing network.

W32.HLLW.Gaobot.BB (Win32 Worm): This is a variant of W32.HLLW.Gaobot.AE that attempts to spread to network shares that have weak passwords, and allows access to an infected computer through an IRC channel. The worm also attempts to terminate the processes of various antiviral and firewall programs. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is packed with Petite.

W32.HLLW.Gaobot.BC (Win32 Worm): This is a variant of W32.HLLW.Gaobot.BB that attempts to spread to network shares that have weak passwords, and allows access to an infected computer through an IRC channel. The worm also attempts to terminate the processes of various antiviral and firewall programs. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is packed with Petite.

W32.HLLW.Gaobot.BE (Aliases: W32.HLLW.Gaobot.BD, W32/Gaobot.worm, Backdoor.Agobot.3.h) (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

It is compressed with FSG.

W32.HLLW.Gaobot.BF (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO that attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

It is compressed with UPX.

W32.HLLW.Gaobot.BH (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO that attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

It is compressed with UPX.

W32.HLLW.Gaobot.BI (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is compressed with ASPack.

W32.HLLW.Gaobot.BM (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO that attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.

It is compressed with UPX.

W32.HLLW.Mantas (Win32 Worm): This is a worm that spreads through file-sharing networks and mapped network drives. It overwrites all the txt/doc/html/jpg/gif/ico/bmp and executable files under specific folders, "My documents," and mapped network drives. The existence of the file winmants.exe is an indication of a possible infection.

W32.HLLW.Repeatld (Alias: W32/Generic.worm!p2p) (Win32 Worm): This is a worm that spreads via KaZaA and IRC. The existence of the repeatld.exe file is an indication of a possible infection. It is written in the Microsoft Visual Basic programming language.

W32.HLLW.Reur (Aliases: W32.HLLW.Wanado, W32/Reur.worm!p2p, Worm.P2P.Reur.c) (Win32 Worm): This is a worm that spreads through the eMule file-sharing network. It is written in Borland Delphi and is packed with FSG.

W32.HLLW.Theug (Win32 Worm): This is a worm that spreads using common file-sharing applications, such as KaZaA, Limewire, and Morpheus. It disguises itself using different file names.

W32.HLLP.Zodiak (Win32 Virus): This is a virus that prepends itself to all the .exe files in the Windows installation folder. It is written in the Microsoft Visual Basic programming language and is compressed with tElock.

W32/Holar-I (Aliases: I-Worm.Hawawi.g, Win32/Holar.I, W32/Holar.l@MM, W32.Galil.C@mm, WORM_HAWAWI.F) (Win32 Worm): This worm has been reported in the wild. It is an internet worm which spreads via file sharing on peer-to-peer networks and by e-mailing itself to addresses found on the local computer in such places as the Outlook address book and TXT, HTML, HTM, and EML files. The worm may arrive in an e-mail using various subject lines. The name of the attached file will be that of the executing worm. W32/Holar-I searches the registry for the path to the KaZaA share folder and will copy itself to that location with a PIF, EXE, COM, BAT, or SCR extension. An example would be: <Drive letter>:\Program Files\KaZaA\My Shared Folder\Kazaa.bat. W32/Holar-I will also copy itself to the Windows system folder using the executed worm filename with a .SYS extension. Other files created in the Windows system folder, that may also be copied to the Windows temp folder, include explore.exe, smtp.ocx, and a.pif (can also have EXE, BAT, SCR or COM extension). The file smtp.ocx is a legitimate software component and therefore detection is not included for this file. The following registry entry is created to ensure the worm is activated at system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Explore = <Drive letter>:\%system%\explore.exe

The default Internet Explorer start page registry entry is changed to:

- HKCU\Software\Microsoft\Internet Explorer\Main\Start Page = http://www.geocities.com/yori_mrakkadi

The following registry entries are added for the purposes of infection marker and payload timing respectively:

- HKLM\Software\Microsoft\Windows\a
- HKCU\DeathTime

The registry entry HKCU\DeathTime stores a counter of the number of times W32/Holar-I has been run. When the value of this registry entry reaches 30, the computer will stop responding to input and the following message will be displayed over the entire screen in red on a black background: "! have noth!na say bam st!ll ZaCker !"

W32.Jermy.A (Aliases: IRC/Jeremy.A, Wom32/VBTrojan.gen, I-Worm.Kazus.c) (Win32 Worm): This is a simple worm that is written in Visual Basic. It attempts to send itself to the addresses in the Microsoft Outlook Address Book; however, examples we have seen fail in this functionality due to bugs in its code. The intended e-mail has a variable subject and an attachment named either 3DText.scr or Kernei32.exe. It also attempts to connect to a predefined IRC server to await instructions from its authors.

W32.Kwbot.R.Worm (Aliases: Worm.P2P.SpyBot.gen, W32/Spybot.worm.gen) (Win32 Worm): This is a worm that attempts to spread through the KaZaA file-sharing network and network shares with weak passwords. It also has backdoor Trojan capabilities, which allows a malicious user to gain control of a compromised computer. It is a variant of W32.Kwbot.Worm and is packed with Petite.

W32.Kwbot.Y.Worm (Aliases: Backdoor.SdBot.12, W32/Kwbot.Worm.C, Win32/Kwbot.B.worm) (Win32 Worm): This is a worm that attempts to spread through the KaZaA file-sharing network. It also has backdoor Trojan capabilities, which allows a malicious user to gain control of a compromised computer. It is a variant of W32.Kwbot.Worm and is packed with FSG.

W32.Mafeg (Aliases: Bloodhound.W32.1, Worm.Win32.Dupate.4180, W32/MGF) (Win32 Worm): This is a memory-resident, file-appending worm that attempts to spread itself through shared network resources. The size of the infected file is increased by 4,180 bytes. When W32.Mafeg is executed, it inserts the Dxupdate.exe file to the %System% folder and adds the value, "Dxupdate.exe"="Dxupdate.exe." to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

If the system is Windows NT/2000/XP/Server 2003, it will attempt to infect the C:\NTLDR file. It also attempt to infect Windows Portable Executable (PE) files when they are executed and scans all the shared folders on the local network. If found, the worm attempts to copy itself to the Startup folder of the remote computer.

W32/Marq-A (Aliases: I-Worm.Voltan, Win32/Marq.A, W32.Marque@mm, W32.Marque.Worm, W32/Marque.worm) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm that works by sending an e-mail containing a link to a webpage which, when activated, will reportedly cause the worm to be downloaded as zelig.scr. At the time of analysis, the webpage in question was not available to confirm the reports. The e-mail will have the following characteristics:

- Subject line: Il momento e' catartico
- Attached file: There will be no attachment to the e-mail.

The text "poesie catartiche" in the message text contains the link to the page that is reported to download the worm. W32/Marq-A sends the e-mail to all entries in the user's Windows Address Book. It also changes the marquee screensaver on Windows to contain the text "A volte ti sento cos vicinia...A volte ti sento cos lontana...Certo che hai proprio un cellulare di merda!." When the worm has run, a webpage (different to the one contained in the link in the e-mail) will be opened. This page was also unavailable at the time of analysis.

W32/Mimail-C (Aliases: W32/Mimail.C@mm, I-Worm.NetWatch, W32/Bics@mm, W32.Bics.A, Mimail.C, WORM_MIMAIL.C) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via e-mail using addresses harvested from the hard drive of the infected computer. All e-mail addresses found on the computer are saved in a file eml.tmp in the Windows folder. In order to run automatically when Windows starts up, W32/Mimail-C copies itself to the file netwatch.exe in the Windows folder and adds the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NetWatch32

The e-mails sent by the worm have the following characteristics:

- Subject line: Re[2]: our private photos <random letters>
- Attached file: photos.zip

W32/Mimail-A spoofs the 'From' field of the sent e-mails using the e-mail address james@<your domain>. Photos.zip is a compressed file that contains an executable file named photos.jpg.exe.

W32/Mimail.D@mm (Aliases: Trojan.Sefex, W32/Mimail@MM, I-Worm.Mimail.d, WORM_MIMAIL.D, Worm/Mimail.B) (Win32 Worm): This memory-resident Internet worm propagates via email using its own SMTP (Simple Mail Transfer Protocol) engine. It sends out email in the following format:

- From: admin@%n%
- To: %n%
- Subject: your account %n%
- Attachment: message.zip
  (Note: %n% denotes a variable string.)

This worm exploits two vulnerabilities, known as Object Tag code base exploit and MHTML exploit, to automatically execute. The vulnerabilities affect the following software:

- Microsoft Outlook Express 5.5
- Microsoft Outlook Express 6.0
- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.5
- Microsoft Internet Explorer 6.0

It runs on Windows 95, 98, ME, NT, 2000, and XP.

W32/Mimail.E@mm (Alias: WORM_MIMAIL.E): (Win32 Worm): This worm is similar to its other variants. It is a memory-resident, multithreaded Internet worm that propagates through email using its own Simple Mail Transfer Protocol (SMTP) engine. The email arrives in the following format:

- Subject: don't be late! &lt8 random characters>
- Attachment: readnow.zip (readnow.doc.scr) &lt8 random characters>

This malware performs a Denial of Service (DoS) attack against the following Web sites.

- www.spews.org
- www.spamhaus.org
- www.spamcop.net

It is packed using UPX program, and runs on Windows 95, 98, ME, NT, 2000, and XP.

Win32/Mimail.F@mm (Aliases: WORM_MIMAIL.F, I-Worm.Win32.Mimail.10784.B) (Win32 Worm): This worm has been reported in the wild. It is similar to its other variants, this worm propagates through email using its own Simple Mail Transfer Protocol (SMTP) engine. The email message it sends out contains the following details:

- Subject: don't be late! &lt8 random characters>
- Attachment: readnow.zip (readnow.doc.scr) &lt8 random characters>

It also performs a denial of service (DoS) attack against the following Web sites.

- www.mysupersales.com
- www.mysupersales.net
- mysupersales.com
- mysupersales.net

It is UPX-compressed and runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_MIMAIL.G (Aliases: Win32:MiMail-E4, I-Worm.Win32.Mimail.10784.C, Worm/Mimail.F, Mimail.F@mm, Win32.HLLM.Foo, W32.Mimail.C@mm, W32/Mimail@MM, Win32/Mimail.gen, I-Worm.Mimail.f) (Win32 Worm): This is a memory-resident worm that randomly launches a Denial of Service attack against the following Web sites:

- fethard.biz
- fethard-finance.com
- www.fethard.biz
- www.fethard-finance.com

Like the earlier variant, WORM_MIMAIL.A, it propagates by sending itself via email to addresses it gathers from certain files found on the infected system. It runs on Windows 95, 98, ME, NT, 2000, and XP.

W32/Mimail-H (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads via email using addresses harvested from the hard drive of the infected computer. All email addresses found on the computer are saved in a file named eml.tmp in the Windows folder. In order to run itself automatically when Windows starts up the worm copies itself to the file cnfrm33.exe in the Windows folder and adds the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Cn323

The emails sent by the worm have the following characteristics:

- Subject line: don't be late!<30 spaces><random characters>
- Attached file: readnow.zip

W32/Mimail-H spoofs the From field of the sent emails using the email address john@<your domain>. Readnow.zip is a compressed file that contains an executable file named readnow.doc.scr. The worm also creates a copy of itself named exe.tmp and a copy of readnow.zip named zip.tmp, both in the Windows folder. W32/Mimail-H will occasionally generate and send corrupted copies of readnow.zip. While searching for email addresses in files on the local hard drive W32/Mimail-H attempts to exclude files that have various extensions. W32/Mimail-H also attempts denial of service attacks targeting:

- spamhaus.org
- www.spamhaus.org
- spews.org
- www.spews.org

W32/Opaserv-R (Win32 Worm): This is a variant of W32/Opaserv-A. It spreads via network shares. The worm will copy itself into the Windows folder on the current drive and add the following registry entry so that it is run when the system starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Brasil= C:\Windows\Brasil.pif

It attempts to copy itself to the Windows folder on networked computers with open shared drives. The worm then modifies the win.ini on the remote machine to ensure it will be run on system restart. It also attempts to download files and drop the files put.ini, brasil.dat, and brasil!.dat to the root folder of the current drive.

W32.Randex.R (Win32 Worm): This is a network-aware worm that spreads itself through shared network drives as the file, Service.exe. It receives instructions from an IRC channel on a specific IRC server. One such command triggers the aforementioned spreading. W32.Randex.R may open ports 20, 113, 445, 1024, 55808. It also opens randomly chosen ports.

W32.Randex.S (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author.

W32.Remabl.Worm (Win32 Worm): This is a worm that attempts to spread through the local network and may have backdoor capabilities. The existence of the file shambl3r.exe is an indication of a possible infection.

W32.Sakao (Alias: W32.HLLW.Sakao) (Win32 Virus): This is a simple virus that attempts to spread itself through floppy disks. It is written in the Microsoft Visual Basic (VB) programming language. The VB run-time libraries are required for W32.Sakao to be executed. Due to a bug in the code, the file name and location of the virus must be one of the following:

- \Sadako.exe
- A:\Sadako.exe
- C:\WINDOWS\Start Menu\Programs\Startup\FindFast.exe
- \Myfile
- A:\Myfile.exe
- C:\WINDOWS\File.exe

W32/Sober-A (Aliases: I-Worm.Sober, Win32/Sober.A, W32.Sober@mm, Win32.HLLM.Odin, Worm/Sober, Win32/Sober.A@mm, I-Worm.Win32.Sober, I-Worm/Sober.A, W32/Sober.A.worm, WORM_SOBER.A) (Win32 Worm): This worm has been reported in the wild. It is an e-mail worm with various subject lines, message text and attachments. W32/Sober-A creates three copies of itself in the Windows system folder. One of the filenames is always similare.exe and other two filenames are randomly chosen (e.g. systemchk.exe, systemini.exe). W32/Sober-A adds a filename to the following registry entry so that the worm runs when you logon to your computer:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

W32/Sober-A creates the following file underneath the Windows system folder: Macromed\Help\Media.dll. This file contains e-mail addresses collected from the system. It is not malicious and can be deleted. W32/Sober-A employs a technique that will cause the virus to be restarted if its process is terminated.

W32/Torvil.d@MM (Aliases: I-Worm.Torvil.d, W32.HLLW.Torvil@mm) (Win32 Worm): This mass-mailing worm spreads via e-mail, open fileshares, P2P sharing applications, Internet Relay Chat, and Usenet newsgroups. It also attempts to terminate security software, and exploits the MS02-015 vulnerability. It may be received in an e-mail message with a wide variety of subject lines, message bodies, and attachment names. The from address may be spoofed, or forged. When the attachment is run, a dialog box is displayed. If the Exit button is pressed, the virus installs itself and the box goes away. If the Patch button is pressed, an installation simulation occurs, followed by another message box. The virus copies itself to the WINDOWS directory using the name spool or smss followed by 2 random characters, followed by .exe. A registry key is created to load that file at startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Service Host" = %WinDir%\spool (random characters) .exe

A WIN.INI run key is created to load the worm as well. On WinNT/2K/XP this results in the following key getting set:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon "Shell" = Explorer.exe spool (random characters) .exe

The worm installs itself as a service with the following parameters:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TORVIL
  Description = Provides Local Access to the Registry
  DisplayName = System Registry Service
  ImagePath = (path to worm) xStartOurNiceServicesYes

Registry changes are made to automatically execute the worm each time a .bat, .cmd, .com, .exe, .pif, or .scr file is run.

- HKEY_CLASSES_ROOT\batfile\shell\open\command "(Default)" = C:\WINNT\svchost.exe "%1" %*
- HKEY_CLASSES_ROOT\cmdfile\shell\open\command "(Default)" = C:\WINNT\svchost.exe "%1" %*
- HKEY_CLASSES_ROOT\comfile\shell\open\command "(Default)" = C:\WINNT\svchost.exe "%1" %*
- HKEY_CLASSES_ROOT\exefile\shell\open\command "(Default)" = C:\WINNT\svchost.exe "%1" %*

- HKEY_CLASSES_ROOT\piffile\shell\open\command "(Default)" = C:\WINNT\svchost.exe "%1" %*
- HKEY_CLASSES_ROOT\scrfile\shell\open\command "(Default)" = C:\WINNT\svchost.exe "%1" /S

Several additional registry keys are created to hide system files, disable registry editing, and for the worm to track its progress.

- HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced "ShowSuperHidden"=0
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System "DisableRegistryTools"=1
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System "DisableRegistryTools"=1
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\OneLevelDeeper

Two files are created in the Windows directory for the worm to use when spreading. The virus saves many copies of itself to a hidden directory named:Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D} within the Windows directory. Filenames contained in this directory are derived using three methods. Various extensions (.EXE, .PIF, .SCR) may be appended to filenames used during this process. Dropped .HTM files contain MIME encoded copies of the worm, followed by Exploit-CodeBase code to automatically execute the virus when a file is accessed on an unpatched system. The worm sends itself to e-mail addresses harvested from files containing the various strings. It uses MAPI to retrieve information stored in exiting messages, and references the Outlook Express stationary, possibly to alter the default stationary, setting it to a dropped message.htm file containing the worm. The worm also contains its own SMTP engine to send messages. It attempts to gain access to remote systems through the various shares. Numerous passwords are used in an attempt to gain access. The worm calls the NetScheduleJob API to create a scheduled task remotely; executing itself on the target system remotely. The worm also copies itself to the Xolo, KaZaA, and eDonkey2000 shared directories. It overwrites the mIRC.INI file to send itself to users who join the same channel as the infected user. The worm carries a long list of Usenet newsgroups and server names, which it uses to post infectious messages.

W97M.Rochitz.C (Aliases: Macro.Word97.Rochitz, W97M/Generic) (Word 97 Macro Virus): This is a variant of W97M.Rochitz.A, which is a macro virus that infects Microsoft Word documents. The virus infects documents when they are opened or closed.

WORM_ARRET.A (Aliases: W32/Lohack.C.worm, W32.Lofni.Worm, W32/Noala, I-Worm.Ticton, i-worm.WinSux, W32/Ticton-A, Win32.Noala.B, W32/Noala.b@MM) (W32 Worm):
This Win32 worm spreads via e-mail using SMTP (Simple Mail Transfer Protocol) and via network shares. It gathers e-mail addresses from the following sources:

- Windows Address Book
- List of contacts in NET Messenger
- Web pages found by Google (www.google.com) based from query strings found inside the worm's body

The worm then sends out an e-mail message with a varying subject, message body, and attachment file name to all the e-mail addresses it finds. It exploits a known vulnerability in Microsoft Outlook or Outlook Express that allows e-mail attachments to automatically execute when an e-mail message is opened or viewed in the preview pane. This worm also spreads across the network by searching for network shared folders with write access. It drops copies of itself to these shared folders using various file names. This UPX compressed worm is written and compiled in Visual Basic. It affects Windows 95, 98, ME, NT, 2000 and XP.

WORM_MOEGA.C (Internet Worm): This malware has both worm and backdoor capabilities. To propagate, it scans for hosts in the affected system's domain. This worm then drops a copy of itself in target hosts, which have shares with weak passwords. As a backdoor, it connects to a remote Internet Relay Chat (IRC) server and joins a channel. Once it is in the IRC channel, a malicious user can then send commands, which the malware executes on the compromised machine. It runs on Windows NT, 2000 and XP systems.

Worm/Napsin (Alias: I-Worm.Napsin) (Internet Worm): This is a memory resident Internet worm that attempts to spread through e-mail by using addresses it collects in the Microsoft Outlook Address Book. However- it does not successfully send itself. If executed, the worm copies itself in the \windows\%system% directory under the filename "SINAPPS.EXE." It was originally received as "Sinapps.exe."

WORM_SEXER.B (Aliases: Win32.HLLM.Nicky.3, I-Worm.Sexer.c, W32/Sexer.worm, W32.Wintoo.B.Worm, I-Worm.Sexer) (Internet Worm): This mass-mailing worm propagates by sending a copy of itself to all the e-mail addresses found in the Windows Address Book (WAB) using an e-mail message with the following characteristics:

- From: Kaspersky Lab &ltsupport@kaspersky.com>
- Subject: Утилита для выявления и удаления почтовых червей
- Attachment: KAVUtil.exe

The malware code is packed with PKLite and developed in Delphi, a high-level programming language. It runs on Windows 95, 98, ME, NT, 2000, XP and 2003.

Worm/Spybot.12904 (Alias: I-Worm.SpyBot.12904) (Internet Worm): This is a memory resident Internet worm that copies itself in the as "AUTOUPDATE.EXE" under \windows\%sysdir%\. The sent out e-mail will have the following characteristics:

- Subject: Microsoft Security Update
- Attachment: MS03-047.EXE

So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "windowsupdate"="autoupdate.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"windowsupdate"="autoupdate.exe"

WORM_YAHA.AA (Aliases: W32.Yaha.AE@mm, W32.Yaha.AA@me) (Internet Worm): This variant of the YAHA worm attempts to propagate via e-mail and shared network drives. It terminates running antiviral-related processes and tries to launch Denial of Service (DoS) attacks against some specified Web sites. It also prevents users from running certain system applications, including Registry Editor and the Task Manager. To propagate via e-mail, this worm uses its own Simple Mail Transfer Protocol (SMTP) engine to send copies of itself to addresses obtained from different sources. It also logs keystrokes and sends them to a certain e-mail address. It runs on Windows 95, 98, ME, NT, 2000 and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	CyberNotes-2003-18
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
Afcore.q	N/A	CyberNotes-2003-20
AIM-Canbot	N/A	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	CyberNotes-2003-18
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Coreflood.dr	Dr	CyberNotes-2003-19
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.CrashCool	N/A	CyberNotes-2003-19
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Daemonize	N/A	CyberNotes-2003-21
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.DMSpammer	**N/A**	**Current Issue**
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Evilbot.B	B	CyberNotes-2003-19
Backdoor.Evilbot.C	**C**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Backdoor.EZBot	N/A	CyberNotes-2003-18
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.Frango	**N/A**	**Current Issue**
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Graybird.G	G	CyberNotes-2003-19
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hazzer	N/A	CyberNotes-2003-20
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hogle	**N/A**	**Current Issue**
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Bot.B	**B**	**Current Issue**
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	CyberNotes-2003-19
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	CyberNotes-2003-19
Backdoor.IRC.Tastyred	N/A	CyberNotes-2003-20
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	CyberNotes-2003-19
Backdoor.Jittar	N/A	CyberNotes-2003-21

Trojan	Version	CyberNotes Issue #
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lassrv	N/A	CyberNotes-2003-21
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Lixy	N/A	CyberNotes-2003-21
Backdoor.Lixy.B	**B**	**Current Issue**
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MeteorShell	N/A	CyberNotes-2003-21
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.Mprox	N/A	CyberNotes-2003-20
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Mxsender	N/A	CyberNotes-2003-21
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Omygo	N/A	CyberNotes-2003-19
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peeper	N/A	CyberNotes-2003-20
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09

Trojan	Version	CyberNotes Issue #
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Pspider.310.b	310.b	CyberNotes-2003-18
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	CyberNotes-2003-18
Backdoor.Ranck	N/A	CyberNotes-2003-18
Backdoor.Ranck.C	**C**	**Current Issue**
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remocy	**N/A**	**Current Issue**
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Roxy.B	B	CyberNotes-2003-20
Backdoor.RPCBot.E	E	CyberNotes-2003-19
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.SDBot.Q	Q	CyberNotes-2003-21
Backdoor.Sdbot.R	R	CyberNotes-2003-21
Backdoor.Semes	N/A	CyberNotes-2003-20
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	CyberNotes-2003-18
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sincom	N/A	CyberNotes-2003-21
Backdoor.Sinit	N/A	CyberNotes-2003-21
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Smokodoor	N/A	CyberNotes-2003-21
Backdoor.Smother	N/A	CyberNotes-2003-20
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	CyberNotes-2003-18
Backdoor.Stealer	N/A	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Surdux	N/A	CyberNotes-2003-20
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Translat	N/A	CyberNotes-2003-20
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	CyberNotes-2003-18
Backdoor.Usirf	N/A	CyberNotes-2003-21
Backdoor.Uzbet	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wollf.16	16	CyberNotes-2003-18
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zombam.B	B	CyberNotes-2003-20
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12

Trojan	Version	CyberNotes Issue #
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
Backdoor-AZF	AZF	CyberNotes-2003-20
BackDoor-BAE	BAE	CyberNotes-2003-21
BackDoor-BBO	**BBO**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/PowerSpider.A	A	CyberNotes-2003-11
BDS/SdBot.76870	76870	CyberNotes-2003-21
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	CyberNotes-2003-19
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	CyberNotes-2003-19
Desex	N/A	CyberNotes-2003-20
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Magicon	**N/A**	**Current Issue**
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	CyberNotes-2003-19
Downloader.Dluca.C	C	CyberNotes-2003-20
Downloader.Dluca.D	**D**	**Current Issue**
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader.Slime	N/A	CyberNotes-2003-21
Downloader.Tooncom	**N/A**	**Current Issue**
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
DownLoader-EG	EG	CyberNotes-2003-20

Trojan	Version	CyberNotes Issue #
Downloader-ES	**ES**	**Current Issue**
Downloader-EU	**EU**	**Current Issue**
Downloader-EV	**EV**	**Current Issue**
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Enocider	**N/A**	**Current Issue**
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.Keysteal	N/A	CyberNotes-2003-19
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IgetNet.dr	dr	CyberNotes-2003-21
IRC.Trojan.Fgt	**Fgt**	**Current Issue**
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Fortnight.D	**D**	**Current Issue**
JS.Seeker.J	J	CyberNotes-2003-01
JS.Seeker.K	K	CyberNotes-2003-20
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Mico	N/A	CyberNotes-2003-20
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MouseLog-Ladora	**N/A**	**Current Issue**
MultiDropper-FD	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
OF97/ExeDrop-B	N/A	CyberNotes-2003-19
Pac	N/A	CyberNotes-2003-04
Petala	N/A	CyberNotes-2003-20
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
Proxy-Regate	**N/A**	**Current Issue**
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Bugmaf	N/A	CyberNotes-2003-21
PWS-Mob	**N/A**	**Current Issue**
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Bancos.C	**C**	**Current Issue**
PWSteal.Banpaes	N/A	CyberNotes-2003-21
PWSteal.Finero	N/A	CyberNotes-2003-21
PWSteal.Firum	**N/A**	**Current Issue**
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Lemir.E	E	CyberNotes-2003-20
PWSteal.Lemir.F	F	CyberNotes-2003-20
PWSteal.Nikana	N/A	CyberNotes-2003-21
PWSteal.Reanet	N/A	CyberNotes-2003-21
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Salira	N/A	CyberNotes-2003-21
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWSteal.Tarno	**N/A**	**Current Issue**
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial15	**15**	**Current Issue**
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
StartPage-U	U	CyberNotes-2003-20
StartPage-W	**W**	**Current Issue**
Stealther	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	CyberNotes-2003-19
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	CyberNotes-2003-19
Troj/Bdoor-AAG	AAG	CyberNotes-2003-21
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/CoreFloo-C	**C**	**Current Issue**
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Eyeveg-A	A	CyberNotes-2003-19
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hackarmy-A	A	CyberNotes-2003-20
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Ircbot-M	M	CyberNotes-2003-21
Troj/IRCBot-P	**P**	**Current Issue**
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13

Trojan	Version	CyberNotes Issue #
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qhosts-1	N/A	CyberNotes-2003-20
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Webber-A	A	CyberNotes-2003-15
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Abaxo	N/A	CyberNotes-2003-20
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Bootconf	N/A	CyberNotes-2003-21
Trojan.Boxer	N/A	CyberNotes-2003-19
Trojan.Cuydoc	N/A	CyberNotes-2003-21
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Gaslide.Intd	N/A	CyberNotes-2003-20
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.Kalshi	N/A	CyberNotes-2003-21
Trojan.KillAV.B	B	CyberNotes-2003-19
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Loome	**N/A**	**Current Issue**
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Mumuboy.B	B	CyberNotes-2003-20
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Myss.B	B	CyberNotes-2003-21
Trojan.Norio	N/A	CyberNotes-2003-19
Trojan.Obsorb	**N/A**	**Current Issue**
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.PWS.QQPass.E	E	CyberNotes-2003-20
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Retsam	**N/A**	**Current Issue**
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Sinkin	N/A	CyberNotes-2003-21
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Vardo	N/A	CyberNotes-2003-20
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
TrojanGaslid	N/A	CyberNotes-2003-18
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Adclicker.G.Trojan	**G**	**Current Issue**
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Tofazzol	**N/A**	**Current Issue**
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
W97M.Tabi.Trojan	N/A	CyberNotes-2003-20
Woodcot	N/A	CyberNotes-2003-16
X97M.Sysbin	**N/A**	**Current Issue**
Xin	N/A	CyberNotes-2003-03

BackDoor-BBO (Alias: Backdoor.Kutex): This is a remote access Trojan written in Delphi. It might come with an installation exe. Upon execution, the installation exe copies the Trojan into the %Windir% directory as messenger.exe. (Where %Windir% is the Windows directory, for example C:\WINDOWS). The installation exe creates the following registry key to hook system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Messenger-" = "%Windir%\Messenger.exe"

Once running on the victim machine, the Trojan component opens TCP sockets accepting commands sent from the malicious user on port 9696, 3000. The Trojan connects to login.icq.com as ICQ client.

Backdoor.DMSpammer: This is a Backdoor Trojan Horse that relays spam e-mail messages. It is usually found as the file, C:\Program Files\Common Files\MSDM\msdm.exe. When Backdoor.DMSpammer is executed, it listens on a (configurable) port for spammers, who can send it a list of addresses.

Backdoor.Evilbot.C: This is a variant of Backdoor.Evilbot that allows unauthorized access to an infected computer. It could also allow a malicious user to launch a remote attack using an infected computer. When Backdoor.Evilbot.C runs, it copies itself as %Windir%\WinServ.exe and adds the following value, "AKEYNAME"="%Windir%\WinServ.exe," to registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Backdoor.Frango: This is a Backdoor Trojan Horse that gives a malicious user unauthorized access to a computer. It is packed by FSG. The Trojan notifies the malicious user by ICQ and CGI requests and listens on port 23435, by default.

Backdoor.Hogle: This is a proxy SMTP server that may be used as an anonymous spam relay. It also listens on TCP port 3355 for incoming connections.

Backdoor.IRC.Bot.B (Aliases: Backdoor.IRC.Bot, BackDoor-BBB, BKDR_FOLLA.A): This is a Backdoor Trojan Horse that uses the IRC channels to launch Denial of Service (DoS) attacks, and that allows the Trojan's creator to control your computer. The functions of the files may change. This variant of Backdoor.IRC.Bot.B has been reported to have been sent by e-mail. The messages have the following characteristics:

- Subject: hey, stop send letters to me!
- Attachment: Wmdvm.exe

Backdoor.Lixy.B: This is a Backdoor Trojan Horse that opens a proxy server and allows unauthorized access to an infected machine. Backdoor.Lixy.B consists of one .dll file and two .exe files. The file names are usually the following:

- Rgsock32.exe: For setting up and running other Trojan files.
- Msm32.exe: Contains the main routine of the backdoor.
- Ssocks32.dll: A malicious Browser Helper Object that runs Msm32.exe.

When Backdoor.Lixy.B is executed, it adds the following keys to the registry:

- HKEY_CLASSES_ROOT\CLSID\{1E1B2879-88FF-11D2-8D96-000000000004}
- HKEY_CLASSES_ROOT\HTMLEdit.SSocks32
- HKEY_CLASSES_ROOT\HTMLEdit.SSocks32.1
- HKEY_LOCAL_MACHINE\Software\CLASSES\CLSID\{1E1B2879-88FF-11D2-8D96-D7ACAC95951A}HKEY_LOCAL_MACHINE\Software\CLASSES\HTMLEdit.SSocks32
- HKEY_LOCAL_MACHINE\Software\CLASSES\HTMLEdit.SSocks32.1
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Browser Helper Objects\{000000000004}

which adds Ssocks32.dll as a Browser Helper Object. The Trojan starts a proxy server and opens TCP ports 1029-1084.

Backdoor.Ranck.C (Aliases: TROJ_RANCK.A, TrojanProxy.Win32.Ranck, Proxy-FBSR): This is a Trojan Horse that runs as a proxy server. It is written in Microsoft Visual C++ and is packed with ASPack. When Backdoor.Ranck.C is executed, it opens TCP port 41934, so that it can receive commands from remote malicious users. It runs as a proxy server on a compromised machine and adds the value, "rngmf" = "<path to trojan>," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

Backdoor.Remocy: This is a Backdoor Trojan Horse that gives its creator full control over a computer through a Web browser. When Backdoor.Remocy runs, it drops %System%\Inject.dll and adds the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\rmtSvc

The Trojan opens TCP port 7776, which gives a remote malicious user unobstructed access to a computer through a Web browser.

Download.Magicon: This is a Trojan Horse that downloads files from a predetermined Web site. When Download.Magicon runs, it creates the folder, %Windir%\wintrim, and copies itself as the following files:

- Wintrim.exe
- Uninstall.exe

The Trojan enumerates the running processes on the computer. If one of following processes is found, the Trojan will quit.

- Symproxysvc.exe
- Smc.exe
- Persfw.exe
- Zonealarm.exe
- Blackice.exe

Downloader.Dluca.D (Alias: TrojanDownloader.Win32.Dluca.a): This is a variant of the Downloader.Dluca Trojan Horse that sends information about your computer to a specific Web site.

Downloader-ES (Alias: BS_COREFLOOD.B): This Trojan is in the wild. Reportedly, web sites were hacked such that encoded JavaScript (detected as JS/Cisp) was appended to the end of web pages. This JavaScript created an IFRAME that was loaded with the content from a remote page (on the goling2003.com domain). This content included a malformed OBJECT DATA tag, which exploits the MS03-040 vulnerability. The exploit allowed for the automatic execution of the file INF.OOO (the downloader trojan). This Trojan exists as VBScript, which used FTP to retrieve 2 file and execute them.

- STOP.BAT
- AP216.EXE

Downloader-EU: This Trojan attempts to download a file named BrowserHelper.DLL from the domain madfinder.com. This file is no longer present. When the downloader is run, it copies itself into the WINDOWS SYSTEM32 directory using the filename SVC.EXE (7.168 bytes). A registry run key is created to load the Trojan at startup:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Run "svc" = C:\WINNT\System32\svc.exe

It creates another key called:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ DownloadManager

Downloader-EV: Upon execution on the target machine, the file installs itself into the application data folder, using a random 4-letter filename. A Registry key is added to execute this file at subsequent system startup - the string name used for this key will vary. For example:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Otss" = C:\WINDOWS\ESCN.EXE

Once running, an attempt to made to connect to a remote server (sought by a DNS request). A HTTP GET request is then sent to the server, passing information such as:

- install, update or warning
- version details
- message

So when first run on a machine, the request indicates that an install is desired. Upon failure to connect to the remote server, the request serves as a warning for the remote server to be checked for content.

Downloader.Tooncom (Alias: TrojanDownloader.Win32.Tooncom): This is a Trojan Horse that downloads the file, Loader.exe, from a Web site, and then executes the file. This Trojan also overwrites the Windows Hosts file, which is used for name resolution.

Enocider: This is a simple Trojan that executes itself before running any other executable file. It is written in Visual Basic. Upon execution, a fake error message is displayed. It installs itself into the %WINDIR% directory as Genocide.exe. The following Registry key is added to run the Trojan instead when any executable file is executed:

- HKEY_CLASSES_ROOT\exefile\shell\open\command "(Default)" = genocide.exe "%1" %*

IRC.Trojan.Fgt (Alias: IRC-Worm.Fagot, Fagot, W32.Petch, W32/Petch.A, WORM_FAGOT.A, W32/Petch.worm!irc): This is a downloaded file that disables firewall and security software. It deletes critical system files and changes the Internet Explorer home page to a pornographic page. A website that was responsible for distributing this threat is no longer available. It is UPX-packed and written in the Delphi programming language.

JS.Fortnight.D (Alias: JS/Flea.A, VBS/Flea-A, JS/Flea@M): JS.Fortnight.D is a Trojan Horse that drops a file, which is then inserted into the default signature of Microsoft Outlook Express. Following this, every time you send e-mail using Outlook Express, the message will contain code that will attempt to go to a specific Web site when the recipient opens the e-mail message. It exploits a Microsoft VM vulnerability using IFRAME tags, with the SRC field set to the address of the Trojan's creator. After a series of redirections, an encoded JavaScript will load an applet containing the exploit. On unpatched systems, various registry keys and Web browser settings will be modified.

MouseLog-Ladora (Aliases: Backdoor.Delf.gi, TROJ_PALAVRA.A): This Trojan captures typed keystrokes and mouse movement, and sends this information to a specified e-mail address. It takes small screen shots of the area directly below the mouse pointer each time a mouse button is depressed. The purpose of this action is to steal password information where passwords are entered in by clicking on images/buttons rather than typing keystrokes. When the Trojan is run, a Window is displayed. When the Installer button is pressed, a message box is displayed. The Trojan copies itself to the WINDOWS directory and creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run "Explorer" = %trojan path%

A keyboard hooking DLL file is extracted to the WINDOWS SYSTEM directory as HDLL.DLL. The date/time, computer name, and username are saved to a file named DATA.TXT in the current directory, which is used in the main report file. A hidden directory named Excel is created. Small screen shots are taken each time the mouse is clicked and saved to this directory. When there are 30 images within the directory, they are compressed into an archive file (ZIP) and e-mailed to the author, along with information saved in the DATA.TXT file. That message is as follows:

- From: patrik [patrik123@terra.com.br]
- To: patrik123@terra.com.br
- Subject: %random characters%_%machine name%_user name%
- X-Mailer: NetMasters SMTP Demo

Proxy-Regate: This is a proxy server Trojan, designed to turn an infected system into an e-mail spam relay. It opens two random IP ports and sends infection notification to the author. When the Trojan is run, it copies itself to the WINDOWS SYSTEM (%SysDir%) directory as syscpy.exe. A registry run key is created to load the Trojan at startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Syscpy" = C:\WINNT\System32\syscpy.exe

The Trojan contacts two anti-spam web sites to verify that the IP address of the infected system has not been blacklisted on abust.net or spamcop.net . Presumably noting that the IP address of the infected system has been blacklisted if/when this is the case. A random TCP port and a random UDP port is opened. Information/notification is posted to a page on a remote website (note: several variants have been discovered, this is a partial list and new variants will likely use other sites).

- spreadeaglehos.com
- 66.28.101.143
- www.viewthissite.com

Information sent to the page was likely entered into a database for future spam use. A remote malicious user must send the appropriate packets to infected systems in order to exploit them.

PWSteal.Bancos.C: This is a Trojan Horse that mimics the online interfaces of certain Brazilian banks to try to steal account information. It is a minor variant of PWSteal.Bancos.

PWSteal.Firum: This is a Trojan Horse that attempts to collect credit card information as it is entered into Web forms. It targets Visa, MasterCard, Eurocard, and American Express and is written in Visual Basic. The Trojan may be found as a file named "system32.exe" in the System directory. By default, this is C:\Windows\System (Windows 95/98/ME), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

PWS-Mob: This is password-stealing Trojan that captures information from the local file systems such as the username and password and sends the information to the author via e-mail. Online e-mail and bank account information (username/password), if locally cached, and local access credentials are particularly vulnerable to this threat. When run, the Trojan copies itself to the C:\Windows\System directory. The following file name is used:

- systray32.exe

It creates a registry run key to load itself at Windows start up.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "systray32 " = "C:\Windows\System\Systray32.exe"

A log file "sys.log " is created in the following path:

- C:\Windows\System\Mob\Zip

This log file holds system information such as username, password, RAM, size of HD, and applications used at time of infection. Additionally this Trojan will search for Brazilian on-line banking information and if found will record the login and password into the log file. The log file is then archived into a Zip format and e-mailed to a remote address. The name format used for the Zip file is "<Username> _ p.zip, where 'Username ' is the actual username used to login to the compromised machine.

PWSteal.Tarno: This is a Trojan Horse that attempts to intercept user names and passwords for a number of Web-based services. It sends the user names and passwords to a certain e-mail address using its own SMTP engine.

QDial15: This is a TAPI dialer that tries to use a connected modem to establish a connection to various high premium rate numbers. This Trojan also creates a shortcut that launches Internet Explorer to point to

a remote URL. Copies of the shortcut are placed on the desktop, as part of favorites and the Start Menu with an icon. It makes no changes to the registry.

StartPage-W: This Trojan is written in MSVC and is designed to modify the settings of the Internet Explorer search engine and main start page. These changes are made through the registry keys:

- Hkey_Current_User\Software\Microsoft\Internet Explorer\Main\
- Hkey_Current_User\Software\Microsoft\Internet Explorer\Search\
- Hkey_Local_Machine\Software\Microsoft\Internet Explorer\Main\
- Hkey_Local_Machine\Software\Microsoft\Internet Explorer\Search\

Two files with identical size and contents but with different names are dropped into the following locations:

- %Windir%\default.css
- %Windir%\Web\win.def

The following registry keys refer to these two files listed above:

- Hkey_Current_User\Software\Microsoft\Internet Explorer\Styles
- Hkey_Local_Machine\Software\Microsoft\Internet Explorer\Styles

The Wini.ini file is modified with the following RUN command:

- run=C:\windows\..Progra~1\Common~1\Micros~1\Msinfo\info32.exe

Finally the Trojan drops or overwrites the file HOSTS within the %Windir%folder so that all Internet traffic destined for auto.search.msn.com is redirected to a different location.

Troj/CoreFloo-C (Aliases: TrojanDropper.Win32.Emaner, CoreFlood.dr, Backdoor.Coreflood): This is a backdoor Trojan that allows a remote intruder to access and control the computer via IRC channels. When the installation executable is run on Windows 95, 98 or ME (or FAT drives), it drops a DLL to the Windows System folder with a filename consisting of seven random characters a-z and an extension of DLL. When the installation executable is run on a Windows NT, 2000 or XP system with an NTFS drive it drops the DLL as an ADS file associated with the Windows System folder (typically <WINDOWS>\System32). The new ADS file will also have a random seven character name with an extension of DLL. The installation executable then launches the DLL component that adds its pathname to the following registry entry, so that it is run automatically each time Windows is started:

- HKLMSoftware\Microsoft\Windows\CurrentVersion\RunOnce\<random filename> = rundll32 %SYSTEM% <random filename>.dll,Init 1
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<random filename> = rundll32 %SYSTEM% <random filename>,Init 1

The DLL component injects itself into the EXPLORER process making it invisible in the Task Manager process list. Troj/CoreFloo-C also has anti-delete functionality which attempts to prevent viral processes from being terminated and resets the above registry entries if they are removed.

Troj/IRCBot-P (Alias: Backdoor.IRCBot.gen): This Trojan has been reported in the wild. It is an IRC backdoor Trojan that allows unauthorized remote access to a compromised computer via IRC channels. It copies itself to the Windows system folder with the filename autoupdate.exe and sets the following registry entries to run this copy of the Trojan when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\windowsupdate
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\windowsupdate

Trojan.Loome: This is a Trojan Horse that drops a .dll detected as Spyware.Look2Me. Then, it ends the Explorer.exe process to load the .dll, which crashes Windows 2000/XP.

Trojan.Obsorb: This is a Trojan Horse that causes Windows to continuously restart the computer at the end of the startup process. Because it is written in Visual Basic (VB), it requires the VB run-time libraries to execute. In addition, Windows must be installed in C:\Windows.

Trojan.Retsam: This is a password-stealing Trojan Horse. There are several variants of this Trojan. It is written in the Microsoft Visual Basic programming language and may be compressed with ASPack.

W32.Adclicker.G.Trojan: When W32.Adclicker.G.Trojan is executed, it imports the file, C:\Windows\System32\Msvbvm60.dll. If the file does not exist, this Trojan will exit. As a result, this Trojan will likely run only on Windows XP computers that have the default installation path. The Trojan copies itself to C:\Windows\Syslaunch.exe and adds the value, "Wardo"="C:\WINDOWS\syslaunch.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

So that the Trojan runs when you start Windows. It also tries to generate requests to various Web sites with a referral program, including:

- www.qksrv.net
- service.bfast.com
- click.linksynergy.com...

W32.Tofazzol: This is a Trojan Horse that spreads by floppy disks. This Trojan remains memory-resident and attempts to delete the wav, jpg, bmp, mp3, dat, and mpg files found on the system. Upon execution, W32.Tofazzol copies itself to %Windir%\Rundl.exe. It periodically checks for the presence of a floppy disk. If one is present, the Trojan copies itself to A:\Pamela_NUD12.jpg.exe. It adds the value, "LoadPowerProfile"="rundl.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

X97M.Sysbin: This is a macro Trojan Horse that attempts to rename all the subfolders in any of the following folders:

- C:\Program Files
- C:\
- D:\
- E:\